European Commission

STUDY ON THE LEGAL PROTECTION OF TRADE SECRETS IN THE CONTEXT OF THE DATA ECONOMY (GRO/SME/20/F/206)

FINAL REPORT

imc FH KREMS UNIVERSITY OF APPLIED SCIENCES / AUSTRIA

BGW Management Advisory Group St.Gallen

KING'S College LONDON

July – 2022

EUROPEAN COMMISSION

Study on the Legal Protection of Trade Secrets in the Context of the Data Economy

Final Report

European Innovation Council and SMEs
Executive Agency (EISMEA)

2022

EUR EA-09-22-449-EN-N

EUROPEAN COMMISSION

European Innovation Council and SMEs Executive Agency (EISMEA)
Unit SMP / SME Pillar, I-02-2: "Competitiveness and Internationalisation"

E-mail: EISMEA-COSME-IP-CALLS@ec.europa.eu

European Commission
B-1049 Brussels

REPORT PREPARED BY

Alfred Radauer, Martin Bader, Tanya Aplin, Ute Konopka, Nicola Searle, Reinhard Altenburger, Christine Bachner

LEGAL NOTICE

This document has been prepared for the European Commission. However, it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

More information on the European Union is available on the Internet (http://www.europa.eu).

Catalogue number: EA-09-22-449-EN-N
ISBN 978-92-9469-425-6
doi: 10.2826/021443

Printed in Belgium

PRINTED ON RECYCLED PAPER

PRINTED ON PROCESS CHLORINE-FREE RECYCLED PAPER (PCF)

List of abbreviations

AI	Artificial Intelligence
API/APIs	Application Programming Interfaces
Art./Arts.	Article/Articles
B2B	Business-to-Business
BEUC	Bureau Européen des Unions de Consommateurs
CAD	Computer Aided Design
CCV	Confidential and Commercially Valuable
CEO	Chief Executive Officer
CJEU	Court of Justice of the European Union
CRM	Customer Relationship Management
DESCA	Development of a Simplified Consortium Agreement
DTSA	Defend Trade Secrets Act
EAM	Enterprise Asset Management
EC	European Commission
ECJ	European Court of Justice
EEA	Economic Espionage Act
EEN	Enterprise Europe Network
EMA	European Medicines Agency
EPO	European Patent Office
ERP	Enterprise Resource Planning
EU	European Union
EUIPO	EU Intellectual Property Office
FDA	Federal Drug Administration
FRAND	Fair, Reasonable And Non-Discriminatory
FTE/FTEs	Full-Time Equivalents
GAFA	Google, Apple, Facebook and Amazon
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IMI	Innovative Medicines Initiative
IoT	Internet of Things
IP	Intellectual Property
IPR/IPRs	Intellectual Property Rights
IT	Information Technology
LI	Life Sciences
M&A	Mergers and Acquisitions
ML	Machine Learning

NDAs	Non-Disclosure Agreements
NGO	Non-Governmental Organisation
OECD	Organisation for Economic Co-operation and Development
OEM/OEMs	Original Equipment Manufacturer
R&D	Research and Development
RMI	Vehicle Repair and Maintenance Information
SCDS	Support Centre for Data Sharing
SEP/SEPs	Standard Essential Patent
SMEs	Small and Medium-Sized Enterprises
SSI	Self Standard Identity
SW	Software
TPM/TPMs	Technical Protection Measures
TRIPS	Agreement on Trade Related Aspects of Intellectual Property Rights
TS	Trade Secrets
TSD	Trade Secrets Directive
TTBER	Licencing Agreements for the Transfer of Technology
TTO	Technology Transfer Office
U.S.	United States
UCPA	Unfair Competition Prevention Act
USP	Unique Selling Proposition
UTSA	Uniform Trade Secrets Act
V2V	Vehicle-to-Vehicle
WEF	World Economic Forum

Table of Contents

Table of Figures

Table of abridged case studies in main text[1]

[1] The full case studies themselves are provided in Annex C.

Executive Summary

***Abstract*: This study analyses a) to what extent the EU legal framework on trade secret protection applies to data which is shared across firms and organisations and b) the application of trade secrets by European firms in practice. It is set against the backdrop of the growing significance of the data economy and data sharing. The study finds that while the significance of data sharing has been and will be increasing, the protection and appropriation of shared data with trade secrets is lagging. Only a few firms are truly familiar with the application of trade secrets in the context of shared data. On the one hand, this might partly be attributed to the rather young age of the EU Trade Secrets Directive (TSD) and still developing IP management practices of many firms that take due account of trade secrets. On the other hand, and because of the lack of developed jurisprudence, many firms are uncertain regarding the exact meaning of some of the terminology which defines trade secrets as well as regarding actual enforceability. Part of this uncertainty can be alleviated through legal reasoning, but some parts may need further clarification or jurisprudence to develop. In practice, trade secrets are used mostly as a second layer of protection after contracts (which are clearly the preferred mode of protection) as well as a tool against misappropriation by third parties with whom no contractual relations exist. The study develops recommendations in the areas of a) operationally improving firm performance when using trade secrets for shared data; b) reducing possible ambiguity and improving clearness when interpreting the TSD; and c) improving and monitoring the legal framework surrounding the use of trade secrets for protecting shared confidential and commercially valuable data.**

Background

- The following document is the Final Report for the "Study on the legal protection of trade secrets in the context of the data economy" (EASME/2020/OP/0008). It examines the use of trade secrets to protect shared confidential and commercially valuable data, and the extent to which trade secrets can be used to facilitate the sharing of such data to foster innovative and business activity.
- The study is set against the backdrop of new technologies like machine learning, Internet-of-Things (IoT) and Artificial Intelligence (AI), plus new technological developments such as machine / sensor generated data, which allow the accumulation of vast amounts of new data. Coupled with today´s and future computing power for processing data sets, and using these in new business models, these developments have led to the notion of data being the "new oil" of the 21st century.
- Against this backdrop, the question of possible rights, including intellectual property (IP) rights and trade secrets, over data has gained significant momentum in recent years. From the different existing types of IP and IP-like instruments, the legal protection provided through trade secrets as per the EU Trade Secret Directive 2016/943 (TSD) – that is any information that is secret; has commercial value because it is secret; and has been subject to reasonable steps to keep the information secret – holds the promise to be a viable tool for protecting and exploiting significant amounts of shared data of strategic importance.
- Hence, this study seeks to answer the following major research questions, the primary question being: To what extent can the legal protection of trade secrets help in creating a safe environment for business-to-business (B2B) data sharing? What are the practices in sharing data that are commercially valuable, confidential, and secret? How are trade secrets used in this context? What are the advantages and loopholes? And eventually: What conclusions and policy recommendations can be derived?

Methodological approach

- Methodology-wise, the study draws on different sources of evidence: a literature review and legal analysis; an interview programme with 51 interview partners; a standardised survey with n=84 responses; and 13 case studies. A focus was placed on four sectors, namely automotive; pharma/life sciences; energy/utilities and financial services. The selection of sectors was done to reflect a certain breadth of business activity and an expected growing significance of data sharing. A multitude of channels were used to find respondents for both the interview programme and survey. First and foremost, the survey was sent to leading European industry associations in the four sectors with the request to forward the questionnaire to their members; several technical associations dealing with data sharing and/or emerging technologies such as connected cars, IoT; direct identification of experts in social networks like linkedin and the promotion of the study herein; or by reaching out to the network of the IP Ambassadors of the Enterprise Europe Network (EEN).

Findings

The following are the major findings:

- The first major conclusion to be drawn from this study is that the topic of data sharing and the commercialisation and protection of data through trade secrets will continue to grow in significance in the future. However, only a small share of companies seems to be currently expert in this specific domain.
- Several factors may explain the situation:
  - Particularly modern ways of data sharing – such as the sharing of big data sets, e.g., for training AI models – seem to be still in their infancy with many industries. Data that is shared seems to involve, in many instances smaller datasets or data incorporating know-how, shared using bilateral contractual agreements, i.e., practices that have been common for longer periods of time.
  - The Trade Secrets Directive (TSD) is a rather new directive; hence, firms have not developed much experience in this regard.
  - In many firms, there seems to be a lack of clear institutional ownership for trade secrets, particularly in connection with data sharing. Different parts of trade secrets are being dealt with by a combination of legal, IP, IT and corporate security departments. Consequently, specific policies governing the use of trade secrets in firms (generally, and even more so in relation to shared confidential and commercially valuable data) seem to have only recently been developed by firms.
- Firms have, therefore, only recently begun to consider the specific roles trade secrets could play in protecting shared confidential and commercially valuable data. In re-organising and adapting their IP policies to the provisions of the TSD, the major use of trade secrets seems to be that of a second layer of protection if/after protection through contracts – which is clearly the most preferred way to regulate data sharing – fails. Trade secrets protection is hence an additional remedy / recourse. It is also deemed useful against misappropriation by third parties, with whom no contractual relationships exist. To a certain degree, trade secrets law may also help in the drafting of contracts by referring to common terminology and concepts.
- The usefulness of "trade secrets protection" is hereby often assumed. In the empirical analysis, there was considerable debate and uncertainty as to the precise meaning of the defining elements of a trade secret, namely about when shared data can be considered commercially valuable to obtain trade secret protection; what is meant by "reasonable steps" to maintain secrecy; and when data (that is shared, perhaps with many parties) can be considered secret. This was often related to the lack of a developed jurisprudence in Europe – a factor that was also discussed in terms of uncertainty regarding the potential to practically enforce trade secrets.
- The legal analysis revealed that some of the uncertainty may not be warranted, if one would consider the reasonings put forward in jurisprudence in other jurisdictions, i.e., in the U.S., where very similar legislation is in place. There are, however, some aspects of the TSD, and the relationship of the Directive to other pieces of legislation (employment law, competition law, criminal sanctions) that merit further discussion, without which the use of trade secrets for facilitating data sharing may be hampered.

- Overall, the evidence as to whether trade secrets protection facilitates the sharing of data or not remains mixed. While there are instances where trade secrets protection has reportedly provided this facilitating role, there have been others where it seems that it can be used to block the sharing of data. A common situation seems to be that many firms, in principle, recognise and would be willing to share data, but at the same time are reluctant to do so, given a) the uncertainties as described above amidst b) a fear that the party who shares the data partly loses control over the data; and/or c) that there is no adequate sharing of benefits and profits, once the party with which the data is shared finds a new way to appropriate the data.
- A look beyond the borders of the EU seems particularly interesting when it comes to the U.S. and Japan. In 2018, Japan revised its Unfair Competition Prevention Act (Act No 47 of 1993) and introduced specific protection for "shared data with limited access". This accounts for situations where trade secrets protection may not be available for machine-generated data (because there are difficulties with satisfying the definition of "trade secret"). While there are detailed guidelines available on how to interpret this new regulation, a viable body of jurisprudence has yet to develop. In the U.S., there is already jurisprudence that could inspire European courts.

Recommendations

There are three sets of recommendations which we have developed:

1. *Operationally improving firm performance when using trade secrets protection for shared confidential and commercially valuable data*

Given the noted scarcity of expert know-how when it comes to trade secrets and data sharing within firms, the most obvious recommendation is to invest in awareness-raising and training in this regard. Respective offerings should seek to develop know-how along two dimensions: legal know-how (also including guidance and interpretation around jurisprudence outside the EU, which could possibly be taken up by European courts) and managerial/process know-how (how to organise the management of confidential information and data in firms, how to govern processes of data sharing).

Given the high significance of contracts in this domain, it is also advisable to create, e.g., contract templates for the sharing of confidential and commercially valuable data governed by trade secrets (in the context of Horizon-Europe, for example, as an additional template along existing contract templates such as DESCA). Company case studies and testimonials may help convey the practicability and importance of the measures to the target audience.

Important multipliers in this regard are, for example, the European IPR Helpdesk (and the international SME helpdesks); the EUIPO (and its awareness-raising and IP observatory activities); national initiatives that foster technology transfer by using IP (like Knowledge Transfer Ireland; or in Austria the National Contact Point IP). The importance of trade secret protection, particularly in the context of data sharing, can also be highlighted in upcoming EU recommendations, such as the revised/amended Codes of Practice for knowledge transfer and valorisation of the EU. Specifically in the context of shared data, bridges and contacts must be sought between the IP community and the mostly technical data sharing community.

2. *Reducing possible ambiguity and improving clearness when interpreting the TSD*

For reducing possible ambiguities and improving the understanding of some of the key features of trade secrets protection – beyond what can be conveyed through awareness raising and training – there are two sets of measures which can be considered: the use of explanatory guidelines as well as direct changes in the TSD itself.

Japan has – of course against a different legal tradition – championed the use of guidelines for trade secrets, and additional guidance can be also found in the U.S. UTSA. While these guidelines cannot be replicated 1:1 in Europe, it seems nonetheless worth considering generating a European version of such guidelines (or a respective recommendation) to improve the understanding of the TSD – in the sense of being inspired by the U.S./Japanese examples. Absent developing jurisprudence, it could, for example, be inspired by analogies with the jurisprudence in the U.S. or in Japan, where feasible – for example, when it comes to questions of clarifying the notions of "commercial value" or "reasonable steps".

3. *Improving and monitoring the legal framework surrounding the use of trade secrets for protecting confidential and commercially valuable data*

The study has revealed that successful use of trade secrets law for protecting and appropriating confidential and commercially valuable data relies also on a good interaction of the application of trade secret law with other pieces of law. This relates primarily to three bodies of law:

- *Employment law*: Different Member States may have different regulations regarding post-termination clauses. Cases in point are for example periods of times defined by law which can be applied by employers to restrict the ability of former employees to obtain a new job with a competitor for a certain period – one of the reasons being that the competitors do not get a head start with a new employee who can apply prior know-how (and possibly also use confidential and commercially valuable data) from the former employer in the context of the new job. Such regulations can help strengthen trade secret protection particularly in cases where the value of trade secrets diminishes (fast) with time. It would be interesting to monitor whether different national laws on employment mobility influence the use of trade secrets for confidential and commercially valuable data.
- *Criminal law / sanctions*: Most Member States have (different) criminal sanctions in place for misappropriating IP and/or trade secrets. The Japanese example has shown that a) uncertainty regarding whether certain confidential information constitutes a trade secret or not in conjunction with b) the possibility to fall victim to criminal sanctions may impede the use of trade secrets and/or even data sharing, as a means for employees to stay "on the safe side". Again, it would be interesting to monitor whether such interaction and interdependency between criminal sanctions and the use of trade secrets (more specifically, the sharing of confidential and commercially valuable data protected as trades secrets) can be observed.
- *Competition law*: One – as of now – rather theoretical issue could be if a situation ensures where a certain set of data becomes so valuable in a market that having access to this data becomes a matter of necessity. Hence, the role of a possible "dominant" market player exerting full control over such relevant data and its downstream uses should be dealt with specifically. This situation raises questions of abuse of dominant position and bears some similarity to the situation with standard-essential patents (SEPs), where there is then the obligation to license such patents under FRAND terms. The Data Act Proposal is meant to be a solution to this issue in respect – at least - of machine generated data of interconnected devices that affect aftermarket services for those devices. However, its interface with trade secrets protection needs further consideration.

The situations described above do not necessitate a change to the TSD per se and given that evidence of use of trade secrets and the respective jurisprudence is developing, the issue is more of being aware of the possible problems and monitoring whether they materialise in practice. Post-employment restrictions and criminal sanctions regimes may raise the question of whether harmonisation at EU level is needed. This monitoring function – through, e.g., studies, the implementation of working groups – could be made a task for bodies like the EU´s SCDS.

Résumé analytique

***Résumé* : La présente étude analyse a) dans quelle mesure le cadre juridique européen relatif à la protection des secrets d'affaires s'applique aux données partagées entre organisations et entreprises et b) l'application des secrets d'affaires par les entreprises européennes. L'étude est réalisée dans le contexte de l'importance croissante de l'économie des données et du partage des données. L'étude constate que si l'importance du partage de données croît et continuera de croître, la protection et l'obtention des données partagées contenant des secrets d'affaires est à la traîne. Seule une poignée d'entreprises a une réelle expérience de l'application des secrets d'affaires dans le domaine du partage de données. D'une part, cette situation peut être attribuée au fait que la Directive européenne sur la protection des secrets d'affaires est relativement récente, et que les pratiques de gestion de la propriété intellectuelle tenant compte des secrets d'affaires dans de nombreuses entreprises sont encore en développement. D'autre part, et faute d'une jurisprudence suffisante, de nombreuses entreprises ont des incertitudes quant au sens exact de certains termes définissant les secrets d'affaires et à l'applicabilité effective de ces derniers. Cette incertitude peut être dissipée en partie par un raisonnement juridique, mais certaines parties pourraient nécessiter de plus amples clarifications ou une jurisprudence plus abondante. En pratique, les secrets d'affaires servent principalement de deuxième couche de protection après les contrats (qui sont clairement le moyen de protection privilégié) et sont également un outil contre l'obtention abusive d'informations par des tiers avec lesquels aucune relation contractuelle n'existe. L'étude formule des recommandations visant à a) améliorer les performances des entreprises dans l'utilisation des secrets d'affaires en vue du partage de données b) lever d'éventuelles ambiguïtés et clarifier les notions lors de l'interprétation de la Directive sur la protection des secrets d'affaires, et c) améliorer et surveiller le cadre juridique de l'utilisation des secrets d'affaires pour la protection de données partagées confidentielles et à valeur commerciale.**

Contexte

- Le document qui suit est le rapport final du document intitulé « Study on the legal protection of trade secrets in the context of the data economy » (étude de la protection juridique des secrets d'affaires dans le cadre de l'économie des données) (EASME/2020/OP/0008). L'étude examine l'utilisation des secrets d'affaires pour la protection des données partagées confidentielles et à valeur commerciale, et la mesure dans laquelle les secrets d'affaires peuvent être utilisés pour faciliter le partage de telles données afin de favoriser l'innovation et les activités commerciales.
- L'étude est réalisée dans un contexte où de nouvelles technologies telles que le « machine learning » (apprentissage automatique), l'Internet des objets (IoT) et l'intelligence artificielle (IA), ainsi que de nouvelles évolutions technologiques telles que les données générées par des machines et des capteurs, donnent lieu à une énorme accumulation de données. Associées à la puissance de calcul présente et future des ordinateurs pour le traitement de séries de données et à l'utilisation de ces derniers dans de nouveaux modèles économiques, ces cumuls de données ont inspiré la notion du « nouveau pétrole » du 21e siècle.
- Dans ce contexte, la question des droits possibles sur les données, notamment des droits de propriété intellectuelle et des secrets d'affaires, a pris de l'ampleur ces dernières années. À partir des différents types de propriété intellectuelle ou instruments similaires actuels, la protection juridique conférée par les secrets d'affaire au titre de la Directive européenne 2016/943 sur la protection des secrets d'affaires (c'est-à-dire toute information qui est secrète a une valeur commerciale du fait qu'elle est secrète et pour laquelle des mesures raisonnables ont été prises pour la garder secrète) promet d'être un outil viable pour la protection et l'exploitation de quantités significatives de données partagées ayant une importance stratégique.

- Par conséquent, la présente étude cherche à répondre aux principales questions de recherche qui suivent, la plus importante étant : dans quelle mesure la protection juridique des secrets d'affaires permet-elle de créer un environnement sûr pour le partage de données entre entreprises ? Quelles pratiques ont cours dans le partage de données confidentielles, secrètes et à valeur commerciale ? Comment les secrets d'affaires sont-ils utilisés dans ce cadre ? Quels en sont les avantages et les failles ? Et enfin : Quelles conclusions et quelles recommandations réglementaires peuvent être formulées ?

Méthodologie

- Sur le plan méthodologique, l'étude tire ses conclusions de différentes sources de preuves: une revue et une analyse juridique de la littérature, un programme d'interviews de 51 partenaires, un questionnaire standardisé de n = 84 réponses, 13 études de cas. L'accent a été mis sur quatre secteurs d'activité : l'automobile, l'industrie pharmaceutique et des sciences de la vie, les énergies et les services publics et financiers. Ces secteurs ont été sélectionnés de manière à refléter une certaine variété d'activités commerciales et l'importance croissante attendue du partage de données.
- De nombreux canaux ont été utilisés pour trouver des répondants au programme d'interviews et au questionnaire. Avant tout, le questionnaire a été envoyé aux principales associations industrielles européennes des quatre secteurs avec la demande de le transmettre à leurs membres ; il a été envoyé à plusieurs associations techniques s'intéressant au partage de données et/ou aux technologies émergentes telles que la voiture connectée et l'IoT ; des experts ont été identifiés directement sur les réseaux sociaux tels que LinkedIn et la promotion de l'étude a été faite sur ces plateformes ; les auteurs de l'étude ont pris contact avec le réseau des ambassadeurs de la propriété intellectuelle de l'Enterprise Europe Network (EEN).

Conclusions

Voici les principales conclusions:

- La première des conclusions majeures tirée de cette étude est que la question du partage de données, de la commercialisation et de la protection des données par les secrets d'affaires continuera de gagner en importance à l'avenir. Cependant, seule une faible part des entreprises semble maîtriser actuellement ce domaine spécifique.
- Cette situation peut s'expliquer par plusieurs facteurs :
    - Des modèles particulièrement modernes de partage de données, tels que le partage de grandes séries de données (pour l'apprentissage des modèles d'IA par ex.), semblent en être encore à leurs débuts, et ce, pour beaucoup d'industries. Dans de nombreux cas, les données partagées semblent concerner des séries de données de petite taille ou des données comprenant le savoir-faire, partagées dans le cadre de contrats bilatéraux, c'est-à-dire des pratiques en usage depuis longtemps.
    - La Directive sur la protection des secrets d'affaires est plutôt récente, d'où le peu d'expérience des entreprises en la matière.
    - Pour beaucoup d'entreprises, la propriété institutionnelle des données semble confuse, en particulier concernant le partage de données. En effet, la gestion de différents aspects des secrets d'affaires est partagée entre les services juridique, informatique, de sécurité et de propriété intellectuelle. Par conséquent, ce n'est que récemment, semble-t-il, que les entreprises ont élaboré des politiques spécifiques régissant leur utilisation des secrets d'affaires (surtout concernant les données partagées confidentielles et à valeur commerciale).
- Ce n'est donc que depuis peu que les entreprises considèrent le rôle que peuvent jouer les secrets d'affaires dans la protection des données partagées confidentielles et à valeur commerciale. La réorganisation de leurs politiques de propriété intellectuelle pour les adapter à la Directive sur la protection des secrets d'affaires, constituant généralement en une deuxième couche de protection pour les cas où la protection

offerte par les contrats (qui constituent clairement le moyen préféré de réguler le partage de données) échoue. La protection des secrets d’affaires est donc un recours/remède complémentaire. C’est également un moyen jugé utile pour empêcher des tiers avec lesquels aucune relation contractuelle n’existe, de se procurer abusivement des données Dans une certaine mesure, le droit relatif aux secrets d’affaires peut également être une aide à la rédaction de contrats grâce à une terminologie et des notions communes.

- Ici, l’utilité de la « protection des secrets d’affaires » est souvent supposée. L’analyse empirique a révélé qu’il y avait une incertitude et un débat importants autour du sens précis des éléments caractéristiques d’un secret d’affaires, notamment à quel moment des données partagées peuvent être jugées comme ayant valeur commerciale en vue de leur protection par des secrets d’affaires, le sens de « mesures raisonnables » pour préserver leur caractère secret, et à quand des données (partagées, peut-être entre plusieurs parties) peuvent être considérées comme secrètes. Ce fait était souvent lié à une jurisprudence insuffisante en Europe, un facteur abordé également en termes d’incertitude relative à l’application pratique des secrets d’affaires.
- L’analyse juridique a révélé qu’une partie de cette incertitude n’avait sans doute pas lieu d’être si l’on considère les raisonnements avancés dans la jurisprudence d’autres juridictions, c’est-à-dire aux États-Unis, qui ont une législation très similaire. Toutefois, certains aspects de la Directive sur la protection des secrets d’affaires, et le lien de la Directive avec d’autres textes législatifs (droit du travail, droit de la concurrence, sanctions pénales), méritent une discussion plus poussée, faute de quoi l’utilisation des secrets d’affaires pourrait être limitée.
- Dans l’ensemble, les éléments démontrant le rôle facilitateur de la protection des secrets d’affaires dans le partage des données sont mitigés. Si, dans certains cas, la protection des secrets d’affaires s’est avérée jouer ce rôle, dans d’autre cas, elle semble être un moyen d’empêcher le partage des données Une situation courante semble montrer que de nombreuses entreprises reconnaissent le principe du partage de données et seraient prêtes à partager des données, mais sont réticentes en raison a) des incertitudes expliquées ci-dessus b) de la crainte que la partie qui partage les données en perde en partie le contrôle et/ou c) d'un partage insatisfaisant des avantages et des profits une fois que la partie bénéficiaire des données partagées trouve un autre moyen de les obtenir.
- Un regard au-delà des frontières de l’Union européenne, notamment aux États-Unis et au Japon, semble être d’un intérêt particulier. En effet, en 2018, le Japon a révisé sa loi sur la prévention de la concurrence déloyale (loi no 47 de 1993) et y a introduit des protections spécifiques pour « les données partagées à accès limité ». Cette révision tient compte des situations où la protection des secrets d’affaires est susceptible d’être absente pour les données générées par des machines (à cause de la difficulté à définir les données répondant au « secret d’affaires »). Bien qu’il y existe des directives détaillées relatives à l’interprétation de ce nouveau règlement, il manque un corpus de jurisprudence viable.

Recommandations

Nous avons formulé trois thèmes de recommandations:

1. *Améliorer les performances des entreprises dans la protection des secrets d’affaires et le partage de données confidentielles et à valeur commerciale*

Étant donné la rareté du savoir-faire en matière de secrets des affaires et de partage de données au sein des entreprises, la recommandation la plus évidente est d’investir dans la sensibilisation et la formation. Les différentes offres doivent viser à développer un savoir-faire dans deux dimensions : le savoir-faire juridique (ce qui inclut également des conseils et une interprétation en rapport avec la jurisprudence établie hors de l’UE, laquelle peut potentiellement être adoptée par les juridictions européennes), et le savoir-faire managérial ou relatif aux procédures (comment mettre en place la gestion d'informations et de données confidentielles dans les entreprises, comment régir les procédures de partage de données).

Étant donné la grande importance des contrats dans ce domaine, il est également recommandé de créer, par exemple, des modèles de contrat pour le partage de données confidentielles et à valeur commerciale régies par les secrets d'affaires (dans le cadre d'Horizon Europe, par exemple, comme modèle supplémentaire en plus des modèles de contrat actuels tels que DESCA). Des études de cas et des témoignages d'entreprise peuvent contribuer à véhiculer le caractère pratique et l'importance des mesures auprès du public cible.

Des multiplicateurs importants à cet égard sont, par exemple, IPR Helpdesk (et les services internationaux d'assistance aux entreprises), l'EUIPO (avec l'académie de l'EUIPO ou l´Observatoire européen des atteintes aux droits de propriété intellectuelle), les initiatives nationales de promotion des transferts de technologie via la propriété intellectuelle (telles que Knowledge Transfer Ireland ou, en Autriche, le Point de contact national).

L'importance de la protection des secrets d'affaires, en particulier dans le cadre du partage de données, peut également être soulignée dans les prochaines recommandations de l'UE, telles que les codes de bonne pratique révisés ou amendés pour le transfert de connaissance et pour la valorisation de l'UE, ou dans le projet de loi européenne sur les données. Plus précisément, dans le domaine du partage de données, des liens et des points de contact doivent être créés entre la communauté de la propriété intellectuelle et la communauté des ingénieurs et des scientifiques actifs dans le partage de données.

2. *Lever d'éventuelles ambiguïtés et clarifier les notions lors de l'interprétation de la Directive sur la protection des secrets d'affaires*

Pour dissiper d'éventuelles ambiguïtés et clarifier certains aspects clés de la protection des secrets d'affaires (au-delà de ce qui peut être accompli par la sensibilisation et la formation), deux types de mesure peuvent être envisagés : le recours à des lignes directrices explicatives et des modifications directes de la Directive-même.

Le Japon a défendu (bien sûr, dans le cadre d'une tradition juridique différente) l'utilisation des lignes directrices pour les secrets d'affaires, et d'autres orientations peuvent être tirées du Uniform Trade Secrets Act (UTSA) américain. Si ces lignes directrices ne peuvent être reproduites à l'identique en Europe, il semble néanmoins qu'il serait bon d'envisager la formulation d'une version européenne (ou une recommandation respective) afin de clarifier la Directive sur la protection des secrets d'affaire – dans le sens d'être inspiré par les exemples américains/japonais. Faute de jurisprudence, ces lignes directrices pourraient, par exemple, s'inspirer d'analogies avec la jurisprudence américaine ou japonaise lorsque cela est possible ; par exemple, dans le cas des questions de la clarification des notions de « valeur commerciale » ou de « mesures raisonnables ».

3. *Améliorer et surveiller le cadre juridique de l'utilisation des secrets d'affaires pour la protection de données partagées confidentielles et à valeur commerciale*

L'étude a révélé que la bonne utilisation du droit sur les secrets d'affaires pour la protection et l'obtention de données confidentielles et à valeur commerciale repose également sur une bonne interaction entre l'application du droit sur les secrets d'affaires et d'autres textes juridiques. Cela concerne principalement trois corpus juridiques :

- *Le droit du travail* : Les dispositions relatives aux clauses post-résiliation peuvent varier selon les États membres. Tel est le cas pour : les durées définies par la loi que les employeurs peuvent appliquer pour limiter la capacité d'anciens employés à obtenir un nouvel emploi chez un concurrent, l'une des raisons étant que les concurrents ne doivent pas bénéficier d'un avantage grâce au nouvel employé, lequel pourrait appliquer un savoir-faire (et potentiellement utiliser des données confidentielles à valeur commerciale) obtenu auprès de l'ancien l'employeur dans son nouveau travail. De telles dispositions peuvent contribuer à renforcer la protection des secrets d'affaires, en particulier dans les cas où la valeur des secrets d'affaires diminue (rapidement) avec le temps. Il serait intéressant de savoir si des lois différentes sur la mobilité professionnelle influencent le recours aux secrets d'affaires pour les données confidentielles à valeur commerciale.

- *Droit pénal et sanctions pénales* : La plupart des États membres disposent de sanctions pénales (différentes) pour l'obtention abusive de propriété intellectuelle et/ou de secrets d'affaires. Les retours sur la pratique au Japon ont montré que a) l'impossibilité de savoir avec certitude si des informations confidentielles constituent un secret d'affaire ou non, de même que b) la possibilité de tomber sous le coup de sanctions pénales, peuvent contrarier le recours aux secrets d'affaires et/ou même le partage de données, les employés préférant rester « du côté sûr ». Là encore, il serait intéressant de déterminer si une telle interaction et une telle interdépendance entre les sanctions pénales et l'utilisation des secrets d'affaires (plus précisément, le partage de données confidentielles à valeur commerciale protégées comme secrets d'affaires) peuvent être observées. Dans notre échantillon d'entreprises européennes, les sanctions pénales n'ont pas été signalées comme un problème.
- *Droit de la concurrence* : Un problème plutôt théorique (à ce jour) pourrait être de savoir si une situation peut faire en sorte qu'une série de données acquière une telle valeur marchande que l'accès à ces données devienne une nécessité. C'est pourquoi le rôle d'un éventuel acteur de marché « dominant » exerçant un contrôle total sur des données d'une telle importance et sur leurs utilisations en aval devrait être traité de façon spécifique. Cette situation soulève des questions d'abus de position dominante et est similaire d'une certaine manière à la situation des brevets essentiels aux normes, où il y a une obligation d'obtenir des licences de droits de ces brevets sous des conditions équitables, raisonnables et non-discriminatoires (FRAND). Le projet de loi sur les données est destiné à être une solution à ce problème en ce qui concerne (au minimum) les données générées par des appareils interconnectés ayant un impact sur les services après-vente de ces appareils.

Les situations décrites ci-dessus ne nécessitent aucune modification de la Directive sur la protection des secrets d'affaires proprement dits au vu des preuves récoltées sur l'utilisation des secrets d'affaires et étant donné que la jurisprudence correspondante est en cours d'élaboration. Il s'agit davantage d'être conscient des problèmes potentiels et d'être attentif à leur apparition. Les restrictions postérieures à l'emploi et les régimes de sanctions pénales peuvent soulever la question de savoir si leur harmonisation au niveau européen est nécessaire. Ce travail de suivi (à travers, par exemple, des enquêtes ou la mise en œuvre de groupes de travail) pourrait être attribué à des organismes tels que le Support Centre for Data Sharing (SCDS).

Zusammenfassung

Abstrakt: Die vorliegende Studie analysiert a) inwieweit der Rechtsrahmen der EU zu Geschäftsgeheimnissen auf Daten, die zwischen Unternehmen und Organisationen geteilt werden, anwendbar ist sowie b) die tatsächliche Nutzung von Geschäftsgeheimnissen durch europäische Unternehmen in diesem Kontext. Die Studie ist vor dem Hintergrund der wachsenden Bedeutung der Datenökonomie und des Teilens von Daten zu verorten. Die Ergebnisse zeigen, dass – während die Bedeutung des Teilens von Daten gestiegen ist und weiter steigt –, der Schutz und die Verwertung geteilter Daten mittels Geschäftsgeheimnissen dieser Entwicklung hinterherhinkt. Nur ein kleiner Teil der Unternehmen in der EU hat eine hinreichend tiefe Expertise in der Anwendung von Geschäftsgeheimnissen auf geteilte Daten. Dies kann einerseits dem noch jungen Alter der Geschäftsgeheimnisrichtlinie der EU zugeschrieben werden sowie den sich noch entwickelten entsprechenden IP-Managementpraktiken. Andererseits, und weil höchstrichterliche Entscheidungen fehlen, ist eine Unsicherheit bei Unternehmen zu beobachten, wie einige Bestimmungen der Geschäftsgeheimnisrichtlinie ausgelegt werden sollen, und inwieweit die sich ergebenden Rechte in der Praxis auch durchgesetzt werden können. Teilweise lässt sich die Unsicherheit durch juristische Überlegungen beseitigen, aber es gibt auch Aspekte, die einer weitergehenden Klärung bedürfen, z.B. im Rahmen der sich entwickelnden Jurisprudenz. In der Praxis werden Geschäftsgeheimnisse als mögliches „Sicherheitsnetz" genutzt, falls vertragliche Bestimmungen (Verträge sind das am meisten präferierte Instrument für den Schutz geteilter Daten) verletzt werden bzw. nicht halten. Ein weiteres Motiv ist ein Schutz gegenüber Dritten, mit denen keine vertraglichen Beziehungen hinsichtlich der geteilten Daten bestehen. Die Studie hat Handlungsempfehlungen in drei Bereichen entwickelt: a) für die Erhöhung der operativen Performance von Unternehmen in der Anwendung von Geschäftsgeheimnissen auf geteilte Daten, b) für die Reduktion möglicher Unklarheiten bei der Interpretation der Richtlinie sowie c) hinsichtlich der Verbesserung und des Monitorings des Rechtsrahmens, der für die praktische Anwendung von Geschäftsgeheimnissen relevant ist.

Hintergrund

- Das vorliegende Dokument stellt den Endbericht zur „Studie des rechtlichen Schutzes von Geschäftsgeheimnissen in der Datenökonomie" (EASME/2020/OP/0008) dar. Sie untersucht die Nutzung von Geschäftsgeheimnissen zum Schutz geteilter vertraulicher und kommerziell wertvoller Daten und erörtert, inwieweit Geschäftsgeheimnisse in diesem Kontext verwendet werden können, um das Teilen von Daten zwischen Unternehmen (und damit verbunden das Zustandekommen von Innovationen) zu fördern.
- Die Studie ist vor dem Hintergrund der wachsenden Bedeutung neuer Technologien, wie dem Internet der Dinge oder der Künstlichen Intelligenz, sowie neuen technologischen Entwicklungen wie maschinen- bzw. sensorgenerierten Daten zu sehen, die allesamt die Akkumulation großer Datenmengen ermöglichen. Zusammen mit der heute zur Verfügung stehenden Rechenleistung von Computern, um diese Daten zu analysieren, sowie im Zuge neuer Geschäftsmodelle, hat sich der Begriff der „Daten als das Öl des 21. Jahrhunderts" etabliert.
- Diese Gegebenheiten ziehen Fragen nach sich, inwieweit mögliche Rechte, insbesondere geistige Eigentumsrechte, auf Daten bestehen und/oder begründet werden können. Aus dem Kanon existierender gewerblicher (und hierzu verwandter) Schutzrechte, stechen Geschäftsgeheimnisse (gemäß EU-Richtlinie 2016/943) als vielversprechendes Schutzinstrument für viele Arten geteilter Daten hervor – denn diese schützen Daten in jenem Umfang, als diese Information darstellen die vertraulich sind; kommerziell wertvoll (auf Grund der Vertraulichkeit der Informationen); und adäquate Maßnahmen getroffen werden, um die Vertraulichkeit zu gewährleisten.

- Die Studie versucht dementsprechend, Antworten auf die folgenden Forschungsfragen zu liefern: Inwieweit können Geschäftsgeheimnisse einen sicheren Rahmen für geteilte Daten im B2B Umfeld schaffen helfen? Was sind die zu beobachten Usancen beim Teilen von vertraulichen und kommerziell wertvollen Daten? Wie werden Geschäftsgeheimnisse vor diesem Hintergrund eingesetzt? Was sind Vorteile und Schlupflöcher? Und schließlich: Welche Schlussfolgerungen und Handlungsempfehlungen sind zu ziehen?

Methodik

- Die Studie greift auf einen Mixed-Methods Ansatz zurück: eine Literaturanalyse; eine rechtliche Analyse; ein Interviewprogramm mit 51 Interviewpartner*innen; eine standardisierte Unternehmensbefragung mit n=84 antwortenden Betrieben; sowie 13 Unternehmensfallstudien. Der Schwerpunkt lag auf vier Sektoren: Automotive, Pharma/Life Sciences; Energie und Versorger sowie Finanzdienstleistungen. Die Auswahl der Sektoren erfolgte mit der Intention, eine Vielfalt unterschiedlicher Unternehmensaktivitäten abzubilden, wo für alle Sektoren aber auch vermutet werden konnte, dass das Teilen von Daten essenziell ist. Eine Vielzahl an Kanälen wurde genutzt, um Interviewpartner*innen und mögliche Respondent*innen für die Umfrage zu identifizieren. Zuvorderst zu nennen sind hier zentrale Unternehmensverbände und Interessenvertretungen auf europäischer Ebene in den vier Sektoren, die den Fragebogen an ihre Mitglieder weitergeleitet haben; eine Reihe von Vereinigungen, die sich explizit mit dem Teilen von Daten und/oder Technologiefeldern, wo Datenteilen wichtig ist, beschäftigen (z.B. dem Internet der Dinge); die direkte Identifikation von Expert*innen aus professionellen Netzwerken; oder die Nutzung des Enterprise Europe Networks (EEN) und ihren Botschafter*innen für geistiges Eigentum („IP Ambassadors").

Ergebnisse

Die Studie lieferte folgende Befunde:

- Der erste zentrale Befund ist, dass das Thema des Teilens von Daten sowie die Kommerzialisierung als auch der Schutz dieser Daten durch Geschäftsgeheimnisse in Zukunft an Bedeutung gewinnen wird. Indes ist festzustellen, dass derzeit nur ein kleiner Teil der Unternehmen hinreichend Expertise in dieser spezifischen Domäne aufzuweisen scheint.
- Diese Situation erklärende Faktoren sind unter anderem:
    - Bestimmte neuartige Methoden das Teilens von Daten – wie zum Beispiel das Teilen großer Datenmengen zum Training von Modellen künstlicher Intelligenz – scheinen in vielen Branchen erst am Beginn ihrer Entwicklung zu stehen. Daten, die derzeit geteilt werden, sind in der Folge vielfach kleinere Datensets oder Daten, die betriebliches oder technisches Know-How integrieren bzw. widerspiegeln. Vielfach werden diese Daten nur auf bilateraler Ebene geteilt, das heißt es handelt sich um Praktiken, die schon seit vielen Jahren bestehen.
    - Die Richtlinie zu Geschäftsgeheimnissen ist eine eher neue Richtlinie. In der Folge haben noch nicht viele Unternehmen entsprechende Erfahrungen sammeln können.
    - In vielen Firmen dürfte auch eine klare institutionelle Zuständigkeit für Geschäftsgeheimnisse fehlen, insbesondere wenn es um das Teilen von Daten geht. Verschiedene Aspekte das Geschäftsgeheimnisschutzes werden von unterschiedlichen Abteilungen administriert, so der Patentabteilung, der IT-Abteilung, der Rechtsabteilung oder durch den Werksschutz. In der Folge scheint die Entwicklung spezifischer ganzheitlicher betrieblicher Policies zum Umgang mit Geschäftsgeheimnissen (mehr noch in der Anwendung auf geteilte Daten) vielfach ebenfalls in den Kinderschuhen zu stecken.
- Unternehmen haben daher erst rezent damit begonnen, sich mit der möglichen spezifischen Rolle von Geschäftsgeheimnissen zum Schutz von geteilten vertraulichen und kommerziell wertvollen Daten auseinanderzusetzen. Insofern als betriebliche IP-Strategien entsprechend adaptiert wurden, kristallisiert sich als primäres Motiv zur

Nutzung von Geschäftsgeheimnissen die Nutzung als „Sicherheitsnetz", wenn vertragliche Vereinbarungen zur Nutzung geteilter Daten nicht halten und vertragliche Bestimmungen nicht durchgesetzt werden können, heraus. Geschäftsgeheimnisse bieten in diesem Fall eine alternative Route zur Durchsetzung von Geschäftsinteressen. Ein weiteres Motiv ist der Schutz gegen dritte Parteien, mit denen keine vertraglichen Beziehungen über die geteilten Daten bestehen. Schließlich ist auch zu nennen, dass Geschäftsgeheimnisse in gewissem Umfang dabei helfen können, klarere Verträge zu gestalten, da Begrifflichkeiten und Terminologien standardisiert sind.

- Der Nutzen des Geschäftsgeheimnisschutzes wird hierbei von Unternehmen oft aber nur angenommen. In der empirischen Analyse gab es eine lebendige Debatte und auch eine Unsicherheit darüber, wie bestimmte Termini der Geschäftsgeheimnisrichtlinie interpretiert werden sollen. Dies betrifft vor allem das Konzept wann geteilte Daten als kommerziell wertvoll angesehen werden können; was „adäquate" Maßnahmen sind, damit die Vertraulichkeit gewahrt bleibt; und in welchem Umfang Daten, die mit vielen Partner*innen geteilt werden, überhaupt als vertraulich (geheim) anzusehen sind. Dies kann auch mit noch fehlenden höchstrichterlichen Urteilen in Europa in Verbindung gebracht werden – ein Faktor, der auch hinsichtlich der möglichen prinzipiellen Durchsetzbarkeit von Geschäftsgeheimnissen vor Gericht diskutiert wurde.
- Die rechtliche Analyse hat gezeigt, dass Teile dieser gefühlten Unsicherheit nicht bestehen müssten, wenn auf die Rechtsprechung zu Geschäftsgeheimnissen in anderen Jurisdiktionen wie den USA, die eine ähnliche Rechtslage aufweisen, zurückgegriffen wird. Nichtsdestotrotz gibt es einige Aspekte der Geschäftsgeheimnisrichtlinie, sowie bestimmte Aspekte, die die Beziehung von Geschäftsgeheimnissen zu anderen Rechtsgebieten betreffen, welche weiterer Diskussion bedürfen. Im Fokus stehen hierbei die Rechtsgebiete des Arbeitsrechts, des Wettbewerbsrechts sowie des Strafrechts. Eine funktionierende Interaktion des Geschäftsgeheimnisschutzes mit diesen Rechtsgebieten scheint zentral, um die mögliche Funktion der Geschäftsgeheimnisse zum Schutz geteilter und zur Förderung des Teilens von Daten, sicherzustellen.
- Insgesamt ist die Evidenz darüber, ob Geschäftsgeheimnisse das Teilen von Daten fördern oder behindern, durchwachsen. So gibt es einerseits Fälle, wo Geschäftsgeheimnisse überzeugend dazu beigetragen haben, dass Daten zwischen Unternehmen gewinnbringend geteilt wurden. Umgekehrt gibt es aber auch Fälle, wo Geschäftsgeheimnisse dazu genutzt werden können, um das Teilen von Daten zu verhindern. Eine typische Situation scheint zu sein, dass ein Unternehmen zwar einen Nutzen darin erkennt, Daten zu teilen, a) angesichts der oben beschriebenen Unsicherheiten sowie b) der Angst, die Kontrolle über die geteilten Daten zumindest teilweise zu verlieren und/oder c) fehlender sichtbarer Methoden zur Sicherstellung der fairen Teilung eines sich ergebenden Gewinns/Nutzen – sollte eine Kooperationspartner*in einen neuen Weg finden, die Daten zu verwerten –, vom Datenteilen letztlich absieht.
- Ein Blick über die Grenzen der EU hinaus ist insbesondere hinsichtlich der Situation in den USA und in Japan interessant. In 2018 gab es eine Novelle des japanischen Wettbewerbsrechts (Akt zur Verhinderung des unlauteren Wettbewerbs Nr. 47 aus dem Jahr 1993), welche die Einführung eines spezifischen Schutzes für „geteilte Daten mit limitiertem Zugang" mit sich brachte. Dieser spezifische Schutz zielt auf Situationen ab, wo die Voraussetzungen für den Geschäftsgeheimnisschutz für maschinen-generierte Daten nicht gegeben sind. Zwar gibt es hierzu spezifische Richtlinien wie diese neuen Regelungen angewendet werden sollen, eine zugehörige Rechtsprechung fehlt jedoch. In den USA gibt es hingegen Jurisprudenz (allgemein zu Geschäftsgeheimnissen), welche eine Inspirationsquelle für europäische Gerichte darstellen könnte.

Empfehlungen

Handlungsempfehlungen wurden entlang von drei Dimensionen erarbeitet:

1. *Erhöhung der operativen Performance von Unternehmen in der Anwendung von Geschäftsgeheimnissen auf geteilte Daten, die vertraulich und kommerziell wertvoll sind*

Vor dem Hintergrund der relativen Seltenheit von Expert*innenwissen im Untersuchungsfeld ist die offensichtlichste Handlungsempfehlung in bewusstseinsbildende Maßnahmen und Training zu investieren. Die entsprechenden Angebote sollten versuchen, Wissen entlang von zwei Dimensionen zu entwickeln: Rechtliches Knowhow (dies inkludiert Orientierungs- und Interpretationshilfen unter etwaiger Nutzung ausgewählter Jurisprudenz z.B. in den USA, welche möglicherweise dann auch von den europäischen Gerichten herangezogen werden kann) sowie Management- und Prozess-Knowhow (wie man vertrauliche und kommerziell wertvolle Daten in einem Unternehmen administriert, sowie die Prozesse zum Datenteilen aufsetzt und überwacht).

Vor dem Hintergrund der hohen Bedeutung, die Verträge in diesem Themenfeld einnehmen, ist auch zu überlegen, inwieweit Vertragsvorlagen für das Teilen kommerziell wertvoller und vertraulicher Daten entwickelt werden können, die auf Geschäftsgeheimnisse als Schutzinstrument zurückgreifen (im Kontext der europäischen Rahmenprogramme/Horizon Europe etwaig als Ergänzung zu den DESCA Vertragsvorlagen). Unternehmensfallstudien und Testimonials können helfen, die Praktikabilität und Signifikanz der Maßnahmen dem Zielpublikum klarer zu vermitteln.

Wichtige Multiplikatoren sind in diesem Kontext Organisationen wie der Europäische IPR Helpdesk (sowie die internationalen IPR KMU Helpdesks der EU); das EUIPO (mit dessen bewusstseinsbildenden Angeboten der EUIPO Akademie sowie dem Angebot der europäischen Beobachtungsstelle für Verletzungen von Rechten des geistigen Eigentums); nationale Initiativen (z.B. Knowledge Transfer Ireland; oder in Österreich der National Contact Point IP). Die Wichtigkeit des Geschäftsgeheimnisschutzes, im Speziellen im Hinblick auf geteilte Daten, sollte auch in sich in Entwicklung befindenden Empfehlungen der Europäischen Kommission, zum Beispiel zum Wissenstransfer und zur Wissensvalorisierung, aufgenommen und unterstrichen werden. Zudem müssen auch Brücken gebaut werden zwischen der IP-Community und der meist eher technisch orientierten Data Sharing Community.

2. *Reduktion möglicher Unklarheiten bei der Interpretation der EU-Richtlinie zu Geschäftsgeheimnissen*

Um mögliche Unklarheiten zu reduzieren und um das Verständnis einiger Schlüsselkonzepte des Geschäftsgeheimnisschutzes zu verbessern (hinausgehend über Aspekte, welche mittels Trainings und Sensibilisierungsmaßnahmen vermittelt werden können), sind zwei Ansätze prinzipiell vorstellbar: zum einen erläuternde Richtlinien, zum anderen direkte Änderungen in der EU-Richtlinie.

Japan hat, natürlich vor dem Hintergrund einer anderen Rechtstradition, sich der Nutzung von Richtlinien für die Anwendung von Geschäftsgeheimnissen verschrieben. Zudem gibt es zusätzliche Orientierungshilfe in den USA (im Unified Trade Secrets Act). Zwar können diese Richtlinien und Orientierungshilfen nicht 1:1 in Europa repliziert werden. Indes bietet sich die Nutzung als Inspirationsquelle für die Entwicklung europäischer Versionen solcher Richtlinien ab. Solange es keine europäische Jurisprudenz gibt, könnten diese Richtlinien, zum Beispiel, mit Analogien zur U.S. oder japanischen Jurisprudenz arbeiten, in jenen Bereichen, wo dies als sinnvoll erachtet wird (etwaig hinsichtlich der besseren Abgrenzung der Konzepte eines „kommerziellen Wertes" oder „adäquater Maßnahmen").

3. *Verbesserung und Monitoring des Rechtsrahmens, der für die praktische Anwendung von Geschäftsgeheimnissen relevant ist*

Die Studie hat zudem gezeigt, das eine erfolgreiche Anwendung von Geschäftsgeheimnissen stark von einer effektiven Interaktion mit anderen Rechtsgebieten abhängt. Im Fokus stehen vor allem drei Rechtsgebiete:

- *Arbeitsrecht*: Verschiedene Mitgliedstaaten können verschiedene Regelungen zu Kündigungsklauseln in Arbeitsverträgen vorsehen. Beispielsweise können die nationalen Gesetzgeber unterschiedliche Fristen festlegen, die Arbeitgeber*innen einschränken, wie lange ein etwaiges Wettbewerbsverbot für Arbeitnehmer*innen bestehen kann, wenn diese den Job wechseln. Mit solchen Klauseln soll u.a. verhindert werden, dass der Wettbewerb einen unlauteren Vorsprung lukriert, indem auf das bestehende Knowhow einer neuen Mitarbeiter*in (und möglicherweise die Nutzung vertraulicher und kommerziell wertvoller Daten im Besitz dieser Mitarbeiter*in) zurückgegriffen wird. Entsprechende arbeitsrechtliche Regelungen können, je nach Situation, einen etwaigen Geschäftsgeheimnisschutz stärken, vor allem wenn der Wert eines Geschäftsgeheimnisses (stark) mit der Zeit abnimmt. Es wäre zu beobachten, inwieweit sich die entsprechenden unterschiedlichen arbeitsrechtlichen Regelungen auf die Nutzung von Geschäftsgeheimnissen im Kontext geteilter Daten auswirken.
- *Strafrecht*: in ähnlicher Weise haben die Mitgliedstaaten auch unterschiedliche strafrechtliche Sanktionen, wenn es um die Verletzung von Geschäftsgeheimnissen geht. Das japanische Beispiel hat gezeigt, dass a) eine Unsicherheit dahingehend ob vertrauliche Informationen ein Geschäftsgeheimnis sind in Kombination mit b) der Möglichkeit strafrechtlich belangt zu werden dazu führen kann, dass einzelne Mitarbeiter*innen von Unternehmen vom Teilen von Daten absehen, um auf der „sicheren Seite" zu sein. Wiederum wäre es interessant, regelmäßig zu beobachten, ob eine derartige Interaktion und Interdependenz zwischen strafrechtlichen Regelungen und der Nutzung von Geschäftsgeheimnissen auch in Europa besteht (im Speziellen dann im Hinblick auf geteilte Daten).
- *Wettbewerbsrecht:* Ein, derzeit eher theoretisches, Thema, ist, wenn eine Situation entsteht, wo ein bestimmter Datensatz so wertvoll in einem Markt wird, dass der Zugang zu diesem Datensatz für Marktteilnehmer*innen eine Notwendigkeit darstellt. In so einer Situation müsste man sich mit der Rolle einer dominanten Marktteilnehmer*in, welche die Kontrolle über den Zugang zu den Daten hat, spezifisch auseinandersetzen. Diese Situation führt zu Fragen des Missbrauchs einer dominanten Marktposition und ist nicht unähnlich der Diskussion zu standard-essenziellen Patenten, wo es eine Verpflichtung gibt, solche Patente unter bestimmten Bedingungen (FRAND) zu lizenzieren. Der EU Data Act ist als Lösung für dieses Problem gedacht, zumindest für den Fall von maschinen-generierten Daten und miteinander verbundenen Geräten (im Hinblick auf Aftermarket-Dienstleistungen für diese Geräte). Indes könnte die Schnittstelle zum Geschäftsgeheimnisschutz hier stärker berücksichtigt werden.

Die oben dargestellten Situationen erfordern per se keine Änderung der EU-Geschäftsgeheimnisrichtlinie, insbesondere vor dem Hintergrund, dass sich die entsprechende Jurisprudenz entwickelt. Es geht vielmehr darum, sich möglicher Probleme bewusst zu sein und zu beobachten, inwieweit sich diese Probleme in der Praxis materialisieren. Die arbeitsrechtlichen und strafrechtlichen Überlegungen könnten dahingehend weitergeführt werden, ob – angesichts der beobachteten Praktiken –, eine entsprechende Harmonisierung auf EU-Ebene notwendig wird. Die zu Grunde liegende Beobachtungs-/Monitoringfunktion könnte hierbei zu einem Teil des Aufgabengebietes von Organisationen wie der SCDS der EU gemacht werden.

1 Introduction

1.1 The context

The following document is the Final Report for the "Study on the legal protection of trade secrets in the context of the data economy" (EASME/2020/OP/0008). It examines the use of trade secrets to protect and foster the sharing of confidential and commercially valuable data, and the extent to which trade secrets can be used to facilitate the sharing of such data to foster innovative and business activity.

The study is set against the backdrop that new technologies like machine learning, Internet-of-Things (IoT) and Artificial Intelligence (AI), plus new technological developments such as machine/sensor-generated data, which allow the accumulation of (vast) amounts of new data. Coupled with today´s and future computing power for processing data sets, and using these in new business models, these developments have led to the notion, as stated in a 2017 article in the Economist,[2] of data being the "new oil" of the 21st century. This is already reflected in short-term projections. According to the EU Data Strategy, the global volume of data will grow five-fold from 33 zettabytes in 2018 to some 175 zettabytes in 2025.[3] We will also witness a structural shift: from data stored in centralised computing facilities (in 2018 accounting for 80% of where/how data is processed), to smart connected objects, which will account for 80% of data processing in 2025.

It is therefore of no surprise that the question of who "owns" the data and has control over it to reap economic benefits becomes centre-stage. This becomes particularly paramount when data is shared across different firms and organisations – an increasing necessity in today´s "open innovation" environments.

Against this backdrop, the question of possible rights, including intellectual property (IP) rights and trade secrets, over data has gained significant momentum in recent years. From the different existing types of IP and IP-like instruments, the legal protection provided through trade secrets as per the Trade Secret Directive (TSD) – that is, any information that is secret; has commercial value because it is secret; and has been subject to reasonable steps to keep the secret a secret – holds in the eyes of many the potential to be a viable tool for protecting and appropriating significant amounts of shared data of strategic importance.

Therefore, this study seeks to answer the following major research questions, the primary question being:

- To what extent can the legal protection of trade secrets help in creating a safe environment for B2B data sharing?

From this, the terms of reference ask more specifically:

- What evidence can be found to advise the European Commission ('EC') in policy making on the use of legal protection of trade secrets for data sharing purposes?
- What are the practices in sharing data that is commercially valuable, confidential and secret?
- How are trade secrets used in this context? What are the advantages and loopholes?
- What conclusions and policy recommendations can be derived?

[2] The Economist., 'Fuel of the future – Data is giving rise to a new economy', Briefing 6 May 2017 edition.

[3] European Commission, *A European Strategy for Data,* Brussels 19.2.200, COM (2020) 66 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN.

While all types of data are to be considered, the focus will be on industrial and services data and only to small extents on personal data. Furthermore, the analysis is to be executed predominantly for four industry sectors which all have different data sharing practices (pharma, automotive, energy/utilities, financial services).

The approach and structure of the report is meant to underline the interdisciplinary approach for this study, combining economic and legal analysis. Hence, we aim first, as a baseline, to provide legal and economic foundations. Following that, we create a rationale for the questions we asked in the empirical part (which are mostly economic and managerial questions). Eventually, we have the remaining legal analysis referring to the empirical data as well as to questions of conceptual nature. The legal analysis is therefore split in two parts and is framing the economic/empirical analysis. Readers seeking to study just the legal analysis can read (only) section 3.1.1 and hereafter section 5.

Against this backdrop, the report is structured as follows:

- Section 2 provides the summary of the methodology.
- Section 3 gives a baseline understanding of the study problem including the legal foundations (section 3.1.1, part I of the legal analysis) of the TSD, as well as the existing knowledge regarding the use of trade secrets economic /managerial knowledge of the use of trade secrets in the data economy.
- Section 4 presents the empirical analysis of the data collected in the survey, the interviews and elaborated in case studies
- Section 5 provides for a legal analysis considering the opinions and results of the empirical research in the preceding step and deals also with legal questions of a conceptual nature (part II of the main legal analysis)
- Section 6 provides the conclusion and recommendations.

The annexes cover several data tables and figures, to which reference is made in the text, as well as all case studies in their long form. Abridged versions of some case studies are inserted as text boxes throughout the main report, where appropriate, to support arguments presented.

1.2 Acknowledgements

This study would not have been possible without the many inputs obtained from our interview and discussion partners as well as our survey respondents (and those organisations that helped us distribute the questionnaire for the survey).

In particular, we would like to thank Prof. James Pooley and Dr. Christian Spindler, from our study-internal supervisory board, as well as Prof. Josef Drexl, Prof. Cristina Sappa and Dr. Nikolaus Thumm, from our external peer review board for their valuable comments and inputs.

2 Methodology

2.1 General approach

The methodology employed draws on several different evidence sources. It focusses on four industries – automotive, health/life sciences, energy/utilities, financial services – identified in the proposal as being of interest for the study subject and covering also different types of innovative activities (services vs. product-related).

The different evidence sources are:

- *An interview program:* Interviews were conducted with experts in trade secrets and/or data sharing, using a semi-structured interview guideline. 51 interviews were conducted.
- *A survey (between September 2021 and March 2022):* An online web survey using a standardised questionnaire was implemented. The target group were firms and business associations dealing with trade secrets and data sharing. The survey was deployed using a variety of channels (which were also the channels used to identify interview partners):
  - *Social media,* including the contact network of the researchers involved and that of the European Commission.
  - *Pro-contacting of European industry associations:* In all four sectors, major European industry associations were asked for support and affirmed their support by forwarding the questionnaire and interview requests to their member firms and associations.
  - *Contacting of the EEN, in particular their IP Ambassadors:* All IP ambassadors were contacted and asked to support us with the study.
  - *Contacting through active search of individual experts by the researchers*
  - *Contacting in the professional network of the researchers conducting this study*
- *Case studies* (in total 13) have been developed based on interesting interviews and additional document analysis. Abridged versions of the case studies have been inserted in the main text where appropriate to illustrate and/or deepen arguments made. The full case studies are presented in Annex C. The table below provides an overview of the case studies.
- *Literature research:* The different empirical sources of evidence as described above have been complemented by literature research.

Despite the focus on the four industries, we kept the data collection open for other industries and organisations. In defining the four industries, we employed a rather open ecosystem/value chain approach, by which for example, suppliers in different positions of the value chain for an industry were also considered to be part of that industry. That way we also tried to account for the changing and blurring "borders" of industries due to rapid technological change and business model innovation – an aspect particularly relevant for the subject matter scrutinised in this study.

A further source of evidence was the validation and dissemination workshop for the study with stakeholders in the trade secrets and data sharing sphere.

Table 1 Overview of case studies and their main characteristics

Nr.	Focal feature	Sector	Type of organisation	Type of data shared	Data shared with	Use of TS
1	Firm and its beginning journey into confidential and commercially valuable data sharing and trade secret usage	Utilities (energy)	Large firm	Various	Service Providers Collaboration partners	Yes
2	Company where data is currently mostly shared in the scope of R&D projects	Health	Large firm	R&D data	Research partners, universities, research organisations, customers and funding agencies	Yes (but rarely)
3	OEM automotive supplier illustrating the many different types of confidential and commercially valuable data shared and arguing	Automotive	Large firm	Contracts, production-related data, training data sets for AI	Research partners, universities, research organisations, customers and funding agencies	Yes (but rarely)
4	Pharma firm and its need to combine forces and share data with others so that novel treatments can be created	Health / Pharma	Large firm	Clinical trial data, molecular data, manufacturing data	Research partners, competitors	Yes
5	Insurance company – heavy in data sharing, light with IP and trade secrets	Financial Services	Large firm	Various	e.g., health care organisations	No (of minor importance)
6	Mobility service provider in the automotive sector and its use of trade secrets for protecting dynamic data and fundamental rights	Automotive (mobility services)	Large firm	Location data	Maps data suppliers	Yes
7	Machinery firm in the automotive sector using trade secrets as default protection measure and highlighting the subtle differences between shared confidential data that is trade secret protected and shared confidential and commercially valuable data that is not trade secret protected	Automotive sector (supplier)	Large firm	Production process data / machine-generated	Clients, research partners	Yes
8	OEM firm in the automotive sector stating that data sharing follows investment principle and is not available for sharing “as such”, while also raising antitrust issue as a barrier to confidential and commercially valuable data sharing and trade secret usage	Automotive sector (OEM)	Large firm	Various	Suppliers, partners from other industries (insurance companies)	Yes
9	A banking federation in an EU member State reporting on various data sharing practices, the big issue of personal data protection and the little (but growing) role of IP and trade secrets	Banking federation	Association	M&A data, data to detect crimes, R&D data	Banks, insurance companies, tech firms	Not uniform across sector
10	A bank with lots of confidential and commercially valuable data sharing, use of contracts but no real use of trade secrets	Financial services - banking	Large firm	Company investment data, software code	Finance firms	No

11	Electrical and power engineering firm showcasing how to handle different levels of confidentiality while still climbing the trade secret learning curve	Energy (utilities)	Large firm	Product part data/specifications, sensor-acquired data	universities, research institutions, companies with which collaborations are carried out	Yes
12	Automotive supplier with strong trade secrets policies	Automotive (supplier)	Large firm	Production process data, sensor-generated data from vehicles, product specifications and simulation model data	Clients, R&D partners	Yes
13	Health business running a data trade business and applying trade secrets with different levels of confidentiality	Health business	Large firm	Various	Various	Yes

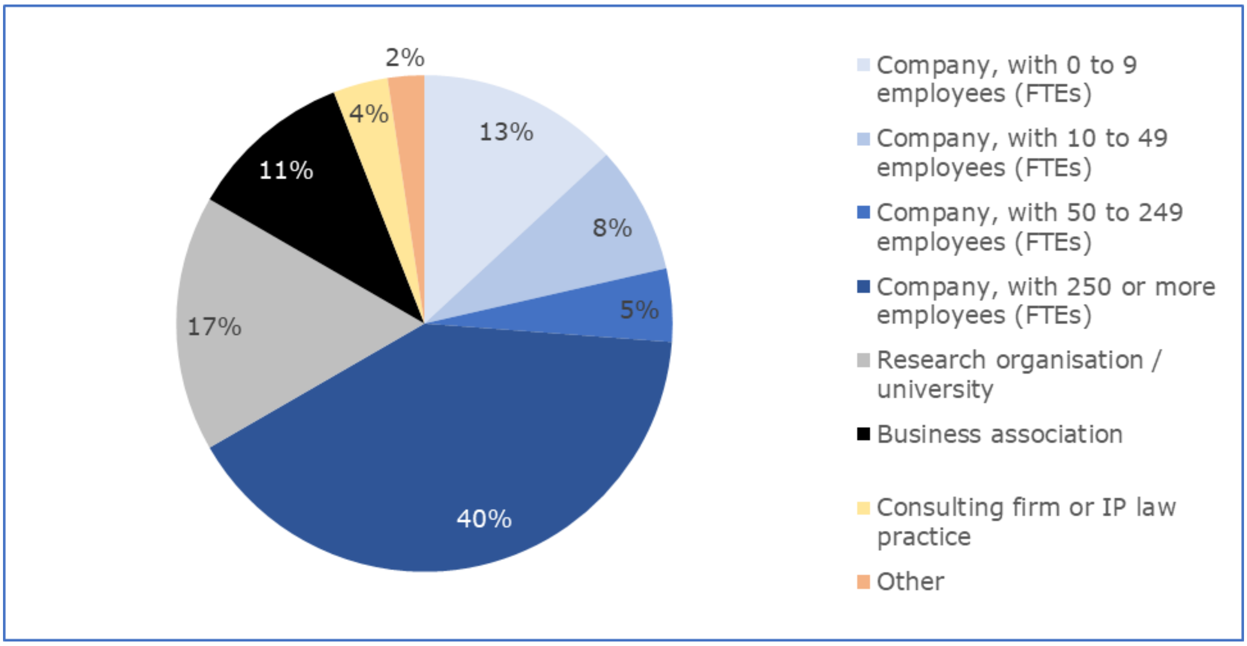
2.2 Survey characteristics

In the following section, we provide information on the survey characteristics. In total, 84 responses could be collected and used for the analysis. This figure falls short of the intended 120 responses, the major reason being – as will be shown in other sections – that the number of firms knowledgeable and "fit" in the combined area of data sharing and trade secret protection was found to be very low. This is, in turn, the result of a) the relative novelty of the TSD (where the managerial implications continue to be absorbed into firms); as well as b) the observation that particularly novel ways of sharing data (e.g., in the realm of big data and AI developments) have also just started to pick up.

This finding is in line also with the qualitative responses of interview partners who had similar observations either about their own firms and/or in their industries. In addition, many industry associations which we contacted (and who also had AI/big data working groups or dedicated IPR working groups) found the study topic interesting but had not yet worked themselves on the topic. In our survey sample, only about 31% were "familiar" with the study topic, while 39% were "rather unfamiliar", "unfamiliar" or did not know how to answer the question on familiarity with TS protection in the context of data sharing (see Figure 17, p. 62). Hence, there were considerable efforts necessary to mobilise respondents.

The following figure shows a breakdown of responses by type of respondents (see Figure 1). As can be seen 40% of the respondents are large enterprises with 250 or more employees. The second largest share is comprised of research organisations, which make up 17% of the sample. Business associations account for 11% of responses. Only a few answers came from consultants (4%) and other types of organisations (2%, which is NGOs).

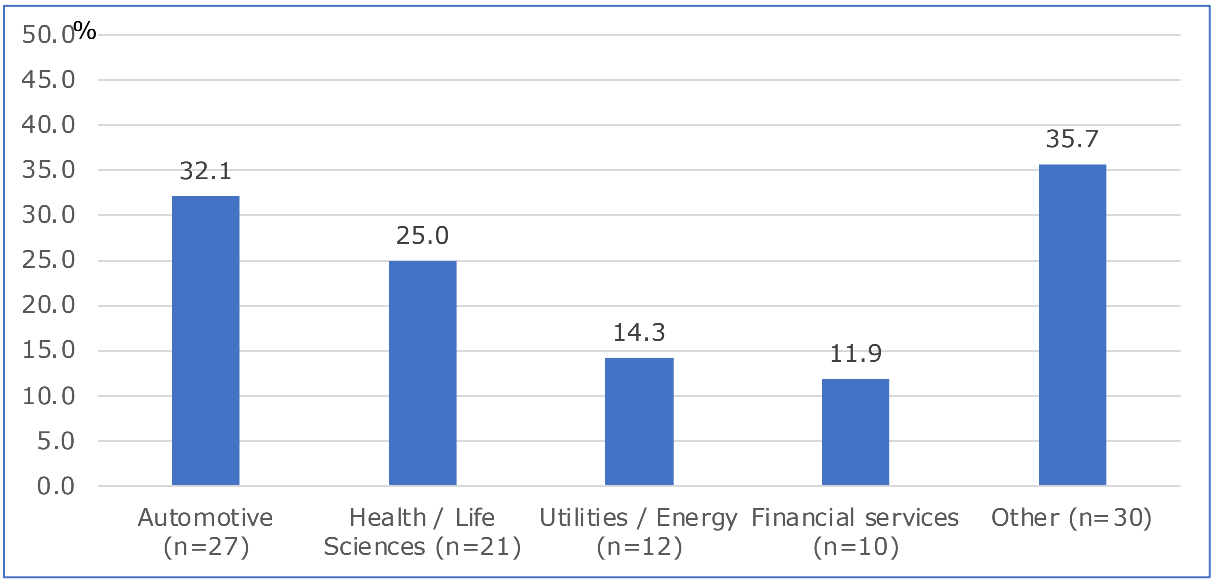
Figure 1 Types of organisations answering the survey, in %



Source: Survey, n = 84

The next figure shows the sectoral breakdown of the responses (see Figure 2). The largest sector is made up of firms from the automotive industry, followed by firms in health and life sciences. Both sectors have enough responses to allow for some statistical analysis. By contrast, the sectors of utilities/energy and financial services have few responses. The large share of firms in other sectors shows the topic of trade secrets and data sharing is important to several industries. In this category, we find companies from the sectors of chemistry, ICT, mechanical engineering, steel making, and semiconductors, amongst others.

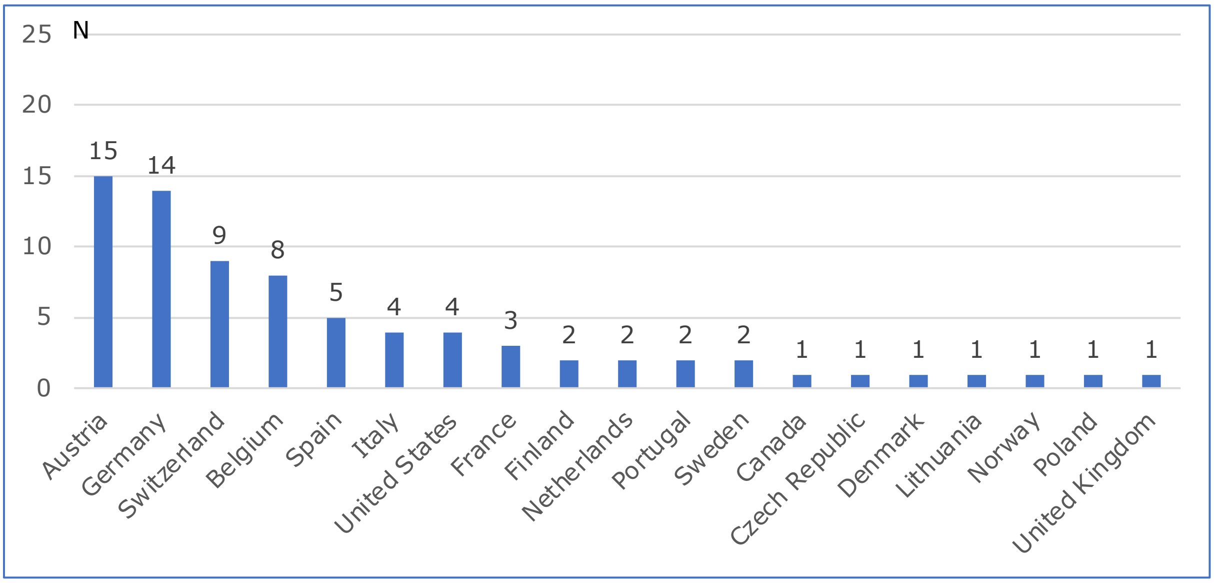
Figure 2 Sectoral breakdown of responses in the sample *)



*) multiple responses allowed
Source: Survey, n= 84

The next figure shows the breakdown of responses by countries (see Figure 3). We observe a bias towards German-speaking countries, which is introduced to the sampling procedure that favoured, to an extent, firms in the network of the research team (also given the challenges to identify viable knowledgeable interview partners). However, it must also be emphasised that Germany is the largest economy in Europe and accounts for around a third of patent applicants at the European Patent Office, for example. Overall, the German-speaking countries make up 49% of the sample of responses. The underlying "n" is reduced from 84 to 77, because seven responses had to be excluded due to apparent lack of validity (Afghanistan, etc. – i.e., errors have been made when entering the responses).

Figure 3 Breakdown of responses by country



Source: Survey, n= 77

3 Legal baseline and the state-of-the art regarding trade secrets use

3.1 The problem at hand

3.1.1 The Trade Secrets Directive (TSD) – legal basics

The EU Trade Secrets Directive 2016/943 (TSD)[4] was adopted to address the problems of legal divergences in the protection of trade secrets in Member States. The benefit of such harmonisation was anticipated to be greater knowledge-exchange between businesses and increased incentives to engage in innovation-related activities in the EU, particularly on a cross-border basis.[5] The TSD is a "generally applicable, technology neutral regime of protection"[6] that protects *"a wide range of know-how and business information"*.[7] Thus, it is a relevant regime to consider in relation to the data economy, although not one that was developed specifically with the concerns of the data economy in mind.

The TSD harmonises key aspects of substantive trade secret law and the enforcement of trade secrets protection. These are minimum standards of harmonisation, thus Member States can exceed what is required by the TSD, provided certain safeguards are met.[8] While the TSD gives Member States flexibility in the choice of civil law mechanism used to implement the harmonised obligations, the protection aligns closest with unfair competition law. Property rights in trade secrets are prohibited.[9]

The harmonisation of substantive law concerns the definition of trade secret, what counts as trade secret misappropriation and lawful acts or exceptions. Article 2 of the TSD defines a trade secret as information that is secret (i.e., is not generally known among or readily accessible to persons within circles that normally deal with the kind of information in question), has commercial value because it is secret, and has been subject to reasonable steps to preserve secrecy.[10] This definition mirrors the requirements of Article 39 on the Agreement on Trade Related Aspects of Intellectual Property Rights 1994 (TRIPS) and also U.S. trade secrets law.[11]

The TSD defines trade secret misappropriation in terms of unlawful acquisition, use or disclosure of trade secrets and infringing goods. Unlawful acquisition occurs where,

[4] [2016] OJ L157/1. Adopted 8 June 2016, with an implementation deadline for Member States of 9 June 2018. For an overview of the Directive and implementation in key member states see Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonisation and Protection of Trade Secrets in the EU* (Edward Elgar, 2020).

[5] See recitals 2-4, 8 TSD.

[6] Drexl, J., *Data Access and Control in the Era of Connected Devices, Study on behalf of BEUC* (2018) available at https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf, p. 91.

[7] Rec. 2, TSD.

[8] See Art. 1 and rec. 10, TSD.

[9] See recitals 1, 16 TSD. See also Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014 on the Proposal of the European Commission for a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure of 28 November 2013, COM (2013) 813 in (2014) 45 IIC 953, [9].

[10] For a general discussion of its ambit see Sousa e Silva, N., 'What exactly is a trade secret under the proposed directive?' (2014) 9 JIPLP 923.

[11] The Uniform Trade Secrets Act (UTSA) was influential when it came to adopting Art. 39 TRIPs: see Sandeen, S.K., 'The limits of trade secret law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on which it is based' in Dreyfuss, R. C. and Strandburg, K. J. (eds) *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (Edward Elgar 2011), ch 20, pp. 554-557.

without the consent of the trade secret holder,[12] there is acquisition by unauthorised access to, appropriation or copy of any materials containing the trade secret, or by any other conduct contrary to honest commercial practices.[13] Unlawful use or disclosure occurs where it is carried out without the consent of the trade secret holder by a person who has unlawfully acquired the trade secret, or in breach of a confidentiality agreement or other duty not to disclose the trade secret; or in breach of a contractual or other duty to limit the use of the trade secret.[14] These unlawful acts can extend to third parties where, at the time of acquisition, use or disclosure, the third party had actual or constructive knowledge that the trade secret was obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully.[15] Article 4(5) of the TSD prohibits commercially dealing in infringing goods, which, according to Article 2(4), are goods whose *"design, characteristics, functioning, manufacturing process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed".* This is a potentially far-reaching provision because there could be a weak causal link between the wrongful misappropriation and the alleged infringing product.[16]

Importantly, certain types of acquisition are declared lawful by Article 3 of the TSD, such as independent discovery or creation and reverse engineering. These are important activities to exclude from trade secret protection, since they help to foster further innovation and competition and ensure the efficacy of the patent system is not undermined.[17] In addition, Article 5 of the TSD specifies that there is no entitlement to remedies for acquisition, use or disclosure of trade secrets in certain circumstances, including in situations where there is an exercise of the right to freedom of expression, and in order to reveal misconduct, wrongdoing or other illegal activity that is in the general public interest. These explicit provisions are seen as especially important protections for whistle-blowers and journalists;[18] however, there are uncertainties about how they should be implemented by Member States and interpreted by courts.[19]

A crucial area that is largely untouched by the TSD is that of employees and ex-employees. Recital 14 of the TSD emphasises that the definition of trade secret does not extend to the *"experience and skills gained by employees in the normal course of their employment"*. Moreover, Article 1(3) stipulates that, *"Nothing in this Directive shall be understood to offer any ground for restricting the mobility of employees"*. In particular, the TSD does not offer

[12] Trade secret holder is defined in Art. 2(2) TSD as "any natural or legal person lawfully controlling a trade secret".

[13] Art. 4(2) TSD.

[14] Art. 4(3) TSD.

[15] Art. 4(4) TSD.

[16] For a critique of Art. 4(5) TSD see: Aplin, T., 'A critical evaluation of the Proposed Trade Secrets Directive' [2014] IPQ 257, pp. 267-269; and Lee, N., 'Protection for artificial intelligence in personalised medicine – the patent/trade secret tradeoff' in J Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar, 2020), ch 14, pp. 269-296, p. 294.

[17] Aplin, T., 'Reverse engineering and commercial secrets' (2013) 66 Current Legal Problems 1, pp. 4–6.

[18] Lapousterle, J., Geiger, C., Olszak, N., & Desaunettes, L., 'What protection for trade secrets in the European Union? A comment on the directive proposal' [2016] EIPR 255, p. 258.

[19] Aplin, T., 'The limits of trade secret protection in the EU' in Sandeen, S., Rademacher, C. & Ohly, A. (eds) *Research Handbook on Information Law and Governance* (Edward Elgar, 2021) ch 10, pp. 174-194 and Mylly, U., 'Freedom of the media and trade secrets in Europe' in Sandeen, S., Rademacher, C. & Ohly, A. (eds) *Research Handbook on Information Law and Governance* (Edward Elgar, 2021) ch 11, pp. 195-216; and Sandeen, S.K. & Mylly, U., 'Trade secrets and the right to information: A comparative analysis of EU and US approaches to freedom of expression and whistleblowing' (2020) 21 North Carolina Journal of Law and Technology 1, available at: https://scholarship.law.unc.edu/ncjolt/vol21/iss3/2.

.

any basis for: (1) limiting employees' use of information that does not constitute a trade secret; (2) limiting employees' use of skills and experience honestly acquired in the normal course of their employment; and (3) imposing any additional restrictions on employees via their contracts that are not in accordance with EU or national law. Thus, it appears that Member States will be left to regulate post-employment situations, including confidentiality and non-compete clauses. This leaves "*the absence of harmonisation on an issue of considerable practical significance*".[20]

In relation to enforcement of trade secrets protection, the TSD harmonises limitation periods, confidentiality during court proceedings, and the remedies available for trade secret misappropriation. Article 8 sets a limitation period of six years for when proceedings for trade secret misappropriation may be brought, but it will be up to Member States to determine when the limitation period begins to run. Article 9 seeks to address the paradox that trade secrets remain valuable and protectable if they are secret and yet court proceedings are inevitably open and public in nature. Thus, a trade secret holder who litigates will inevitably destroy their trade secret by revealing it during court proceedings. Article 9 therefore obligates Member States to ensure that confidentiality is preserved during court proceedings, while at the same time paying due attention to transparency and open justice. Finally, Articles 6 to 7 and 10 to 15 of the TSD deal with the remedies that must be made available where trade secret misappropriation is established. These relate to interim and final measures, along with damages and publication of judicial decisions and comprise an extensive portfolio of measures like those harmonised by the Enforcement Directive.[21] An important feature – and point of contrast with the Enforcement Directive – is that courts must assess the proportionality of provisional measures, injunctive relief and corrective measures according to specific factors that are articulated in the TSD.[22]

Member States have now implemented the TSD (including the former Member State, the UK), although we do see some variations in national implementation.[23] As yet, there have not been any rulings from the CJEU on the TSD, although there has been limited consideration by national courts in Member States of implementation of the TSD.[24] As mentioned above, the TSD is not a data-economy specific form of regulation, but the breadth of the definition of trade secret and the flexible, unfair competition-like form of protection that it offers, means that it may be prove a useful tool.[25]

How the framework of trade secrets protection established by the TSD responds to the concerns of the data economy and whether there should be any reforms to the legislative framework will be analysed in section 5, in light of the empirical evidence that is presented in the subsequent sections 3.1.2 to section 4.

[20] Lapousterle et al., 2016, p. 259.

[21] Directive 2004/48/EC on the enforcement of intellectual property rights, OJ L195/16, 2.6.2004.

[22] See, specifically, Art. 11(2) TSD for provisional and precautionary measures and 13(1) TSD for injunctions and corrective measures.

[23] Compare for example, the discussion of the United Kingdom, Germany, the Nordic countries and Portugal and Spain in Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar, 2020), chapters 5-8.

[24] E.g., in the UK, which was obliged to implement the TSD before its departure from the EU, there has been consideration of national implementation of the TSD in *Shenzen Senior Technology Material Co Ltd v Celgard, LLC* [2020] EWCA Civ 1293, [28] (Arnold LJ). See also De Vroey, M. & Allaerts, M., 'Trade secrets protection: an interim update of Belgian and EU case law' (2021) 16 JIPLP 1391; Germany (2021) 52(6) IIC 775 and Poland (2020) 51(9) IIC 1129.

[25] For an analysis, see Drexl, 2018, pp. 91-106. See also Nordberg, A., 'Trade secrets, big data and artificial intelligence' in Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar, 2020), ch 11, pp. 194-220.

3.1.2 First implications and observations from an economic point of view

As mentioned in the introduction, for new innovations to happen there is an increased need to share data across firm and organisation boundaries. This reveals an on-going paradox of the value of data sharing. To capture value from data, companies share data, often with collaborators and customers. But in doing so, companies must reveal their data for the other party to understand what they are purchasing. The very act of revealing reduces its value, as the other party now has sufficient information to have less need of the data. IP could, according to some authors, be a solution to this paradox, by providing legal protections against the use of proprietary information by third parties.[26]

IP markets will change considerably in the coming years – whereas now traded IP portfolios consist mostly of patents, these technological advances will lead to more diverse IP portfolios (or perhaps better: portfolios of intangible assets), which include IP related to the protection of data (including trade secrets, or copyright), and also data itself.[27] This is remarkable since, while there was previously a discussion aimed at creating a property rights regime for data itself, many believe that data "as such" cannot and/or should not be directly protected by IP.[28]

This does not mean that there are no ways by which some data or certain aspects of data can be indirectly protected. Contract or competition law can regulate access to or use of data in certain ways. To the extent that a database – a collection of independent works, data or other materials arranged in a systematic or methodical way – fulfils the criteria of copyright protection (i.e., being an original creation of a human mind, such as music, video data), the respective arrangement of data would be protected by copyright under the Database Directive.[29] The Directive implements a two-tier protection system. In addition to the copyright protection, "sui generis" database protection as the second tier protects databases, if there has been a significant investment made for creating such databases (obtaining, verification and presentation of data). However, database protection arguably does not apply to the individual elements of the database, i.e., the data itself, but only to substantial parts of the database.[30] And existing case law has been understood as to not confer database protection to databases/collections of data that are a by-product for a company´s main activities.[31]

Given the limitations of the recognised ways to protect data, another type of protection regime has come under the spotlight: trade secrets. Lying between formal and informal protection mechanisms,[32] and already before the advent of the data economy, trade secrets could be considered one of the most important types of IP-like protection. Trade secrets are often a preferred mechanism for companies to protect their innovations and

[26] Arrow, K., 'Economic Welfare and the Allocation of Resources for Invention' in National Bureau of Economic Research, *The Rate and Direction of Inventive Activity: Economic and Social Factors* (1962, Princeton University Press), pp. 609-626.

[27] Donegan, C. & Vella, M., 'IP monetisation: what might the future hold?' in: iam March/April 2019. Accessed via https://www.iam-media.com/article/ip-monetisation-what-might-the-future-hold.

[28] The idea of a data producer´s right was discarded by the EC in 2018. A good argumentation of the shortcomings of a data producer's right is given by Drexl, J., 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) JIPITEC 257.

[29] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases OJ L 77, 27.3.1996, pp. 20–28.

[30] Bently, L., Bodea, G., Calatrava, M.C., Chicot, J., Derclaye, E., Domini, A., Fisher, R., Gkogka, A., Karanikolova, K., Misojcic, M. & Radauer, A., *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases* (2018).

[31] However, a degree of uncertainty exists as to the application of this case law as the EC's evaluation of the Database Directive pointed out.

[32] Trade Secrets are regarded by many as not an IPR, as they do not provide for property over the data but only protect against dishonest misappropriation of the data by third parties. This has a practical consequence in that the IPR Enforcement Directive does not apply. However, one must also note that this may not be entirely consistent with TRIPS which do list trade secrets under the umbrella of IP.

maintain competitive advantages.[33] Firms who report the use of IP protection mechanisms are generally more avid users of trade secrets.[34] There are a mix of conflicting studies which find that different sectors, ages and innovativeness of firms influence the use of trade secrets.[35] The cost of patenting technological inventions, and for maintaining and enforcing patents, are often prohibitive, meaning trade secrets can be a particularly important tool for SMEs.[36]

Consequently, studies[37] show that, amongst firms, trade secrets may be the most preferred way of protecting the intellectual/intangible assets of many companies.[38] Whether this is also the case for the protection of shared confidential and commercially valuable data, is one question under investigation in this study. The recently published results of the EU´s "public consultation on the Data Act and amended rules on the legal protection of databases" suggest, based on responses received from 336 respondents (firms and other types of stakeholders), that *"…the majority of respondents (58%) rely on trade secrets protection when sharing data with other businesses. This figure is higher for business representatives (74%) than for public authorities (24%). Divergences exist between sectors. Some sectors rely heavily on trade secrets protection when sharing data with other businesses (financial: 90%, agricultural: 85%, telecom: 77%). Figures are lower for other sectors, such as the automotive (54%) and the health (57%) sectors. To ensure control over the use of confidential business information, respondents rely on different measures, including contractual arrangements (45%), trade secrets protection (38%), intellectual property rights (31%) and technical means (31%)."*[39]

The definition of trade secrets in the TSD and TRIPS, as described in section 3.1, allows for potentially a large amount of data to be considered for trade secret protection: from information on how to solve a technological problem (every patent is also predated by a

[33] Arundel, A., 'The relative effectiveness of patents and secrecy for appropriation' (2021) 30(4) Research Policy 611–624, available at https://doi.org/10.1016/S0048-7333(00)00100-1; Cohen, W., Nelson, R., & Walsh, J., 'Protecting their Intellectual Assets: Appropriability conditions and why firm patent and why they do not in the American manufacturing sector' (2000) National Bureau of Economic Research Working Paper Series 7552.

[34] Hall, B., Helmers, C., Rogers, M. & Sena, V. (2012). The use of alternatives to patents and limits to incentives, available at https://www.gov.uk/government/publications/the-use-of-alternatives-to-patents-and-limits-to-incentives.

[35] e.g., Holgersson, M., 'Patent management in entrepreneurial SMEs: a literature review and an empirical study of innovation appropriation, patent propensity, and motives' (2013) 43(1) R&D Management 21–36, available at https://doi.org/10.1111/j.1467-9310.2012.00700.x; Leiponen, A. & Byma, J., 'If you cannot block, you better run: Small firms, cooperative innovation, and appropriation strategies' (2009) 38(9) Research Policy 1478–1488, available at https://doi.org/10.1016/j.respol.2009.06.003; Crass, D., Garcia Valero, F., Pitton, F., & Rammer, C., 'Protecting Innovation Through Patents and Trade Secrets: Evidence for Firms with a Single Innovation' (2019) 26(1) International Journal of the Economics of Business 117–156, available at https://doi.org/10.1080/13571516.2019.1553291.

[36] Leiponen & Byma, 2009; Crass, et al., 2019.

[37] See Thomä, J. & Bizer, K., 'To protect or not to protect? Modes of appropriability in the small enterprise sector' (2013) 42 Research Policy 35-49; or Wajsman, N., & García-Valero, F. (2017). *Protecting Innovation through Trade Secrets and Patents: Determinants for European Union Firms*. European Union Intellectual Property Office. European Observatory on Infringements of Intellectual Property Rights. Both studies use CIS data as a basis for their analyses. This latter study already shows that use of trade secrets by industry and sector has been studied, albeit more insights into specifics are still needed.

[38] *"Data economics distinguishes between direct and indirect data trade. Direct trade gives the recipient access to the data. Indirect trade does not transfer any data, only data-driven services. Indirect data trade is by far the most frequent and important data business model. Online advertising, search engines, social media, etc, use this indirect data trade model. This suggests that data secrecy, de facto exclusive control of the data holder through Technical Protection Measures, is indeed the most important form of data trade"* (statement Bertin Martens, JRC).

[39] European Commission, *Public Consultation on the Data Act: Summary Report* (2021), available at https://digital-strategy.ec.europa.eu/en/public-consultation-data-act-summary-report.

trade secret) to non-patentable know-how, as well as things like customer lists (e.g., also personal data). Recital 14 of the TSD indicates the scope of the definition:

> *"It is important to establish a homogenous definition of a trade secret without restricting the subject matter to be protected against misappropriation. Such definition should therefore be constructed so as to cover know-how, business information and technological information where there is both a legitimate interest in keeping them confidential and a legitimate expectation that such confidentiality will be preserved. Furthermore, such know-how or information should have a commercial value, whether actual or potential. Such know-how or information should be considered to have a commercial value, for example, where its unlawful acquisition, use or disclosure is likely to harm the interests of the person lawfully controlling it, in that it undermines that person's scientific and technical potential, business or financial interests, strategic positions or ability to compete. The definition of trade secret excludes trivial information and the experience and skills gained by employees in the normal course of their employment, and also excludes information which is generally known among, or is readily accessible to, persons within the circles that normally deal with the kind of information in question."*

The value of trade secrets has been well-established in academic research. By allowing companies to *not* disclose innovations, trade secrets can provide better and longer protection of innovations compared to patents.[40] Specifically for data, companies may extend the market life of data-generating innovations by bolstering the effectiveness of a patent by maintaining the data as a trade secret, and therefore increasing the cost of reverse engineering to competitors.[41] A classic framing in one of the first papers on the economics of trade secrets, Friedman, et al.[42] argue that companies use trade secrets for innovations of modest value that cannot be independently discovered or reverse engineered within the term of a patent. Generally, companies protect product innovations with patents, as they can more easily be reverse engineered, and process innovations with trade secrets, as they are harder to reverse engineer and detecting patent infringement can be difficult.[43]

An emerging area in both data and trade secrets is the role of cybersecurity. Indeed, as data increases in value, quantity and scope, the protection of this data via trade secrets is ever more dependent on cybersecurity, both in terms of "reasonable steps" to maintain secrecy and protection against breaches. It can be difficult for companies to determine the correct level of investment in cybersecurity, both in terms of meeting legal requirements and the optimal cost-benefit balance. Given the fast pace of technological developments, the threshold for cybersecurity as "reasonable steps" for trade secrecy is volatile,[44] making it a moving target for companies. To optimise investment in cybersecurity, companies need to understand the value of their data, the level of threats and the effectiveness of cybersecurity.[45] Given that all three of those points (value – discussed later in this report, threats and effectiveness) are difficult to measure, it is not an easy task for companies to make these investment decisions. However, cyber breaches can compromise companies'

[40] Anton, J.J. & Yao, D.A., 'Little patents and big secrets: managing intellectual property' (2004) RAND Journal of Economics 1–22

[41] Levine, D.S. & Sichelman, T., 'Why do startups use trade secrets' (2018) 94 Notre Dame L. Rev. 751.

[42] Friedman, D.D., Landes, W. M., Posner, R.A., Journal, T., & Winter, N. 'Some economics of trade secret law' (1991) 5(1) Journal of Economic Perspectives 61–72.

[43] Wajsman & García-Valero, 2017.

[44] Cash, M.H., 'Keep It Secret, Keep It Safe: Protecting Trade Secrets by Revisiting the Reasonable Efforts Requirement in Federal Law' (2015) 23 J. Intell. Prop. L. 263.

[45] Gordon, L.A., & Loeb, M.P., 'The economics of information security investment' (2002) 5(4) ACM Transactions on Information and System Security (TISSEC) 438–457.

competitive advantages by weakening the value of their innovations. Cyber breaches involving the loss of IP negatively impact the stock market performance of victim companies[46] and can cause long-term impact on innovation.[47] More broadly, multiple studies have found the loss of data, including confidential data and trade secrets, is a key cost to companies suffering breaches[48].

In advance of the 2016 Trade Secrets Directive, a substantial report by Martinis, et al.[49] investigated the use of trade secrets by European firms. The study found that manufacturing industries are particularly heavy users of trade secrets protection, and that small firms are at a significant disadvantage in cybersecurity for trade secrets as they lack funds and awareness. A later piece expands on the cybersecurity theme by specifically examining the cyber theft of trade secrets.[50] The authors found that companies are concerned about the rising cyber threat to the integrity of their trade secrets and expect it to become an increasing problem. Another study identified that European companies use trade secrets more than they use patents.[51] Hence, the question of cybersecurity and TPMs must be addressed in the empirical analysis.

Customers, suppliers and collaborators need to have a minimum understanding of the value of data, while the company must balance the value of sharing with the value of protecting their innovations (Arrow's paradox). In collaborative environments, the know-how contained in data facilitates innovation. Companies may be less willing to share data and trade secrets when they are in a leading market position, but companies in weaker positions are more willing to share to demonstrate they are valuable collaborators.[52]

Technological developments bring new types of data into focus: machine-generated data, including also sensor-generated data, in industrial settings; large amounts of (to various degrees personalised) usage data, e.g., on customer preferences and consumer behaviours, mobility data; data that is processed through AI and big data methods (which will result again in new types of data being created). It is the respective "new" types of data that are the focus of this study. Martinis, et al. found companies described data as featuring in both the top three most common types of trade secrets and the most valuable types of trade secrets.[53] It is also clear that at least major types of data will also fall within the remits of trade secret protection, making trade secrets, depending on sector and the type of data, likely an important protection mechanism.

[46] Amir, E., Levi, S. & Livne, T., 'Do firms underreport information on cyber-attacks? Evidence from capital markets' (2018) 23(3) Review of Accounting Studies 1177–1206, available at https://doi.org/10.1007/s11142-018-9452-4.

[47] Andrijcic, E. & Horowitz, B., 'A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property' (2006) 26(4) Risk Analysis 907–923.

[48] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J.G., Levi, M., Moore, T. & Savage, S., 'Measuring the cost of cybercrime' in Brecht, M. & Nowey, T. (eds) *The economics of information security and privacy* (Springer, 2013), ch 12, pp. 265–300; Lagazio, M., Sherif, N., & Cushman, M., 'A multi-level approach to understanding the impact of cyber crime on the financial sector' (2014) 45 Computers & Security 58–74; Wei, H., Frincke, D., Alves-Foss, J., Soule, T., & Pforsich, H., 'A layered decision model for cost-effective network defense' (2005) Information Reuse and Integration, Conf,. IRI-2005 IEEE International Conference On., 506–511.

[49] Martinis, L. de, Gaudino, F. & Respess III, T.S., *Study on Trade Secrets and Confidential Business Information in the Internal Market: Final Study* (April, 2013).

[50] Georgescu, A.-A. E. P., & PWC. (2018). Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber. https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf.

[51] Wajsman & García-Valero, 2017.

[52] Arora, A., Athreye, S. & Huang, C., 'The paradox of openness revisited: Collaborative innovation and patenting by UK innovators' (2016) 45(7) Research Policy 1352–1361, available at https://doi.org/10.1016/j.respol.2016.03.019.

[53] Martinis, et al., 2013.

3.1.3 A first glimpse at data sharing and the strategic role of trade secrets

Apart from the general discussion on ways to protect data via trade secrets (or alternative IP regimes), one also must dive deeper into the necessities and possibilities of *sharing* data among different organisations, such as firms, universities, etc. Typically, data created by one party can (or must be) used by another party to implement or commercialise certain types of innovations. In this open innovation environment, there is a compelling policy objective to increase the possibilities of data sharing across Europe.[54] The respective legislative ways for achieving that are broad and could include: obligations to make certain data publicly available; obligations to make certain data available upon request (comprising also data porting and data portability provisions); obligations to make certain data available to certain stakeholders; exemptions to certain legal protections to rights holders; etc.[55]

Against this backdrop, one can first note the need to strike a critical balance for the protection of shared data, but also the interaction of many pieces of legislation and regulation, partly on top of IP law, referring to data. The Digital Single Market Directive[56] (with explicit provisions on text and data mining), the previously mentioned Database Directive, the General Data Protection Regulation[57], and the proposed Data Governance Act,[58] Digital Markets Act[59] and Data Act,[60] are all examples of "horizontal" means to address data sharing and protection issues across all industries. There are also "vertical", industry specific regulations to be considered, e.g., Directives such as the Open Data Directive[61] (that makes public sector and publicly-funded data re-usable); the Revised Payment Services Directive;[62] data exclusivity in the pharmaceutical sector, whereby clinical trial test data of originator pharma firms is protected for an initial period of up to eight years;[63] in the automotive sector Vehicle Repair and Maintenance Information (RMI)[64]

[54] CapGemini invent, et al., *B2 – Analytical report on EU law applicable to sharing of non-personal data. Support centre for data sharing* (2020).

[55] Ibid. However, it should be underlined that while said obligations arise from the described legal rules, the largest amount of data sharing occurs through voluntary direct or indirect data trade, not subject to obligations but done on a purely market basis.

[56] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC OJ L 130, 17.5.2019, pp. 92–125.

[57] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119, 4.5.2016, p. 1.

[58] Data Governance Act Proposal – see https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0767&from=EN.

[59] Digital Markets Act Proposal - see https://ec.europa.eu/competition-policy/sectors/ict/dma_en.

[60] Data Act Proposal - see https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data.

[61] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information OJ L 172, 26.6.2019, pp. 56–83.

[62] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) OJ L 337, 23.12.2015, pp. 35–127.

[63] de Jongh, T., Radauer, A., Bostyn, S. & Poort, J., *Effects of Supplementary Protection Mechanisms for Pharmaceutical Products*: *Final Report* (2018); technically, this is also compliant with Art. 39(3) TRIPS. See Directive 2011/83/EC of the European Parliament and of the Council of 6 November 2011 on the Community code relating to medicinal products for human use OJ L 311, 28.11.2011, p. 67.

[64] Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information (Text with EEA relevance) OJ L 171, 29.6.2007, pp. 1–16 and Regulation (EC) No 595/2009 of the European Parliament and of the Council of 18 June 2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information and amending Regulation (EC) No 715/2007 and Directive 2007/46/EC and repealing Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC (Text with EEA relevance) OJ L 188, 18.7.2009, pp. 1–13.

and Vehicle Emissions Regulation;[65] in energy the Energy Framework (Clean Energy for All Europeans Package).[66]

Important distinctions are also to be made with respect to personal data and non-personal data. In conjunction with technological developments (e.g., operational requirements) – such as the trend towards the sharing of data dynamically via Application Programming Interfaces (APIs) rather than through static downloads – there is yet another dimension available for managing and protecting access to certain types of data.[67]

Amid these options lie the ways to use trade secrets to protect and manage access to data across organisations. The very design of trade secrets has both conducive and limiting features to data sharing:

- Data cannot be shared too broadly, as then it would eventually not fulfil the requirement that it be secret. The exact thresholds will depend on the facts of the case, i.e., when the data would or would not be "*…generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question."*[68]
- Data also cannot be shared too broadly, as it may undermine the innovations associated with the data (Arrow's paradox). This is also true internally to companies, as the wider data and trade secrets are shared, the more susceptible they are to knowledge leakage.[69] Early academic work suggest firms are less likely to share in fast-developing technology areas.[70] The question arises whether trade secrets are a sufficient means to protect data. After all, trade secrets protect against unlawful/dishonest access to the secret information, e.g., industrial espionage (or misuse of confidential know-how by former employees, for example). This means, for example, that the perfectly legal reverse "engineering" (in the sense of re-creating) of the data – despite considerable investment possibly made in creating the original data – may make trade secret protection less effective in certain cases. On the other hand, appropriation of trade secrets is considered by a significant share of businesses to be of concern, particularly in Europe, where some 20% of firms declare in surveys that they have fallen victim to industrial espionage.[71] It is unclear, however, whether these figures can easily be extrapolated to data being protected with trade secrets. Our research hypothesis is that this may depend on industries, e.g., industries where Europe can be seen as in the lead and where data becomes increasingly important, may be vulnerable – for example, in renewable/wind energy.
- On the other hand, if shared among a somewhat smaller set of trusted partners and with measures in place such as NDAs or cybersecurity (including TPMs) to implement reasonable means to maintain secrecy, trade secrets may be conducive for innovative activities.[72] The OECD notes in this respect: *"…by offering a measure of protection for valuable information and relieving businesses of the need to invest in more costly security measures, some trade secret laws may encourage businesses to invest in the*

[65] Regulation (EU) 2019/631 of the European Parliament and of the Council of 17 April 2019 setting CO2 emission performance standards for new passenger cars and for new light commercial vehicles, and repealing Regulations (EC) No 443/2009 and (EU) No 510/2011 (recast) OJ L 111 25.4.2019, p. 13.

[66] See https://energy.ec.europa.eu/topics/energy-strategy/clean-energy-all-europeans-package_en for details.

[67] CapGemini invent, et al., 2020.

[68] TRIPS Art. 39(2)(a).

[69] Ritala, P., Olander, H., Michailova, S. & Husted, K., 'Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study' (2015) 35 Technovation 22–31, available at https://doi.org/10.1016/j.technovation.2014.07.011.

[70] Appleyard, M.M., 'How does knowledge flow? Interfirm patterns in the semiconductor industry' (1996) 17 Strategic Management Journal 137–154.

[71] Georgescu, 2018.

[72] CapGemini invent, et al., 2020.

development of such information".[73] Particularly, positive impacts on innovation can be argued for if the same legal standards are harmonised for business partners in different Member States.[74] Indeed, some argue that the harmonisation attempts are too little, leaving many loopholes open, to allow for significant cross-border innovation impacts.[75]

- Generally speaking (and not only in relation to collaborations and sharing), there are challenges in valuing trade secrets that may exceed the notable difficulties in valuing other forms of IP such as patents.[76] These challenges are amplified due to the secret nature of the asset, making it difficult for potential collaborators to assess the advantages and risks of data sharing.
- Because protecting data through trade secrets is a rather recent phenomenon in the context of the data economy, there is not much study evidence available on the specific uses of trade secrets,[77] even more so in the context of data sharing. Given the vast amounts of different types of data (personal data vs. non-personal data; machine/sensor- vs. human-generated data, etc.), and the many ways firms experiment in creating business models around data, there is a need for further information to inform policy making.

3.2 Towards the empirics: Specifics of confidential and commercially valuable data sharing

3.2.1 Confidential and commercially valuable data: sharing in general – usage, motives, barriers

After having provided a general baseline, our detailed preparation work for developing the data collection tools started by looking at the questions of usage of confidential and commercially valuable data.

As data has become more important in the economy, so has interest in new ways of doing R&D such as via open innovation.[78] Open innovation, defined by knowledge flowing across organisational boundaries, is associated with higher levels of innovation and improved business performance.[79] Freely flowing knowledge, even within the company, supports innovation.[80]

Companies use trade secrets to manage knowledge flows[81] and data flows. Companies engaged in collaboration with others are heavier users of both patents and trade secrets. This is particularly true when European companies partner with American, Chinese, or Indian firms, where trade secrets are used in 80–83% of collaborations, compared to 38–

[73] OECD, 2019, p.100

[74] CapGemini invent, et al., 2020.

[75] Aplin, 2014. See also Dittmer, S. & Pooley, J. (lead authors). *Protecting Trade Secrets – Recent EU and U.S. reforms* (International Chamber of Commerce, 2019).

[76] http://www.incrementaladvantage.com/articles-objective-analysis/strategic-implications-of-trade-secrets/.

[77] Wajsman & García-Valero, 2017.

[78] Chesbrough, H.W., *Open innovation: The new imperative for creating and profiting from technology*. (Harvard Business Press, 2003).

[79] Chesbrough, H., 'The Future of Open Innovation' (2017) 60(1) Research-Technology Management 35–38, available at https://doi.org/10.1080/08956308.2017.1255054.

[80] King, A. W., 'Disentangling interfirm and intrafirm causal ambiguity: A conceptual model of causal ambiguity and sustainable competitive advantage' (2007) 32(1) Academy of Management Review 156–178, available at https://doi.org/10.5465/AMR.2007.23464002

[81] Wang, R., 'Information asymmetry and the inefficiency of informal IP strategies within employment relationships' (2021) 162 Technological Forecasting and Social Change 120335, available at: https://doi.org/10.1016/j.techfore.2020.120335.

40% of collaborations with other European companies.[82] It is apparent that sharing data and knowledge has much to offer companies and economies. However, returning to Arrow's paradox, data sharing has a double-edged sword for innovative companies by both unlocking and risking innovations and competitive advantages.

Building on this understanding of the value held in data and its sharing, we consulted first with our scoping interview partners. The discussions indicated it would be good as an opener in an interview to enquire into the significance of data in general, and confidential and commercially valuable data in particular for the businesses. A distinction should be made between the current and the future situation. The hypothesis would be that the significance of confidential and commercially valuable data sharing is high and will be increasing in the future.

In terms of motives, it was asserted that the major motivation to share confidential and commercially valuable data was to commercialise these data assets. However, the discussion on motives quickly led, for many interview partners, to more interesting questions on barriers. One interview partner branded the metaphor of the (to-be-shared) confidential and commercially valuable data as *"ore"*, where companies frequently do not know *"how much gold there is in it"* and lacked respective know-how to identify valuable data as well as access to markets. The *"commercialisation"* aspect meets the major motive to keep the data confidential, which is to keep a comparative competitive advantage.

Sector-specific differences were outlined. From the scoping interviews, it could be inferred there was more of the "we have the ore" situation, for example, in the automotive sector. In this sector, it was said that there is a rather low differentiated mindset where to share (e.g., public commons, public value, standards) and where to execute (exclusive value generation), as compared, for example, with the IT/SW sector. Generally, there is a stand-off between OEMs and suppliers / after-market service providers. OEMs (Original equipment manufacturers) would like to have full data autonomy. They follow a strategy where they want to keep all data exclusive to themselves, including data from purchased components from suppliers. The suppliers, in turn, fight for parallel use of data, particularly for after-market businesses and/or for periods after the vehicle warranty periods run out (the typical timeframe was said to be five years). These inputs are fully in line with the insights from literature.[83] The battlefield for these interests seems to be in sector-specific regulation, notably in the discussions of reforms and amendments of the Motor Vehicle Type Approval Regulation and in relation to RMI (repair and maintenance information).

Furthermore, the concept of data co-generation must be underlined. For example, the data collected by cars is co-generated between several parties: the manufacturer, the driver, the manufacturers of car components, car service providers, etc. Each of these parties can have a claim to access and use the data. The manufacturers design the data architecture of the car and protect the data by means of trade secrecy for their exclusive access by means of TPMs. TPMs exclude access by other parties, unless agreed by the OEM. Overall, this leads to the question of whether TPMs can be used to de-facto create "exclusive rights" even when in fact there is no underlying legal right that is protected through the TPMs.

Three EC-sponsored studies stand out when it comes to analysing motives and barriers for the sharing of data:

- The report of Campmas, et al[84] scrutinised the barriers to data sharing in the automotive (mobility) sector, as ever so often in the literature with a focus on the

[82] Wajsman & García-Valero, 2017.

[83] Kerber, W. & Gill, D., 'Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation' (2019) 10 JIPITEC 244.

[84] Campmas, et al. (n.Y.): Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility. EASME/COSME/2018/004.

connected and automated vehicles. The barriers were: personal data protection/GDPR[85]; data ownership and data access rights; liability and interconnected quality of data; strategic barriers imposed by market players to access data; interoperability issues; lack of digital skills. While the report says that *"...who owns the data and what right different parties have to access this data"* is a major challenge, none of the recommendations are specifically geared towards trade secrets (though trade secrets are mentioned as one appropriation regime particularly for non-personal data, and hence a means to declare "ownership").

- Under the same larger EC project, another report with the same aims was made for the sharing of health data.[86] The authors conclude that the main barriers *"…that either already impede data sharing or can potentially have a negative impact on the development of the health data ecosystem, relate to: i) the regulatory framework for data protection and liability applicable across the EU; ii) the need for a trustworthy system for data sharing built on clear accountability mechanisms; iii) the need for more cooperation on common standards and enhanced data interoperability; iv) the need to ensure access to data and lift strategic barriers in the market; and finally v) the need for digital literacy and skills to support the development of the ecosystem."* The barriers are therefore very similar to the mobility/automotive sector; however, trade secrets did not seem to have played a role at all in this study.
- A third study set out to enquire specifically into modes and practices of data sharing across six industries.[87] Using a combination of desk research, a survey and 16 case studies, the study examined a variety of use cases, motives and barriers to data sharing of machine-generated data (with no distinction being made between personal and non-personal data). The study authors found:
  - That the concept of data sharing is not commonly known and fully understood, an issue exacerbated by the use of different terminologies.
  - Despite awareness of this problem, firms share and re-use data among them (and that the significance of sharing will increase in the future).
  - In terms of motives, it is said: *"Both data suppliers and data users share and re-use data with/from other companies to explore the possibility of developing new business models and/or new products and services. Additionally, data suppliers appear to engage in B2B data sharing to establish partnerships with other companies, and to generate revenue from the monetisation of their data. In turn, data users seem to be interested in accessing data from other companies to enhance their catalogue of products and/or services, as well as to improve their internal efficiency."* However, the study also identified a considerable share of missed business opportunities because of *"…lack of sufficient investment in accessing real-time and/or positioning/localisation data from other companies."*
  - Only a small portion of available data was shared and most sharing took place within the business sector.
  - There are technical and legal barriers for data sharing: *"…technical barriers may include lack of interoperability, safety and security requirements, or curation and infrastructure costs. Legal obstacles may entail the uncertainty about "data ownership" and what can be lawfully done with the data, along with difficulties*

[85] The three points of concern were the lack of sector-specific rules in the GDPR (e.g., dealing with consent requirements relating to vehicle-generated data); b) the lack of guidance on how to implement anonymisation techniques; and c) legal fragmentation.

[86] Iacob, N. & Simonelli, F., *Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting the creation of EU-wide B2B health data marketplaces and unified diabetes-related datasets*. EASME/COSME/2018/004.

[87] European Commission, Directorate-General for Communications Networks, Content and Technology, Scaria, E., Berghmans, A., Pont, M., et al., *Study on data sharing between companies in Europe: final report*, Publications Office, 2018, available at https://data.europa.eu/doi/10.2759/354943.

in meeting the legal requirements on data protection in a business-to-business context."

- Success factors identified were: *"Building trust with data users and data suppliers, understanding the demand for data, establishing partnerships, identifying concrete use cases about what can be done with the data, and putting in place simple and user- friendly tools proved to be key success factors for B2B data sharing."*

A general conclusion at this stage was that studies on practices, motives and barriers to the sharing of data hardly explore the connection between trade secret protection and shared data. Emphasising the confidential and commercially valuable / trade secret nature of the study therefore adds a particular viewpoint that has not yet been extensively empirically covered in the literature.

3.2.2 Typologies of shared data

3.2.2.1 The many ways to categorise data

Finding a comprehensive typology for confidential and commercially valuable data that is being shared – particularly for the purpose of defining the questionnaire – proved to be a difficult task, given the many types of data that can be shared. However, it is still necessary to have a reasonably good classification system to analyse the issues at hand in a differentiated manner. The literature acknowledges this issue. For example, a study by Montjoyhe, et al., for the European Commission, states:[88]

> "*First, any* discussion *of access to data must take into account the heterogeneity of data (along many dimensions), of use cases, of desired access conditions, etc. Discussing access to data in the abstract is futile."*

The authors continue, in their study of "competition analysis in the digital era", to draw on a classification system developed by the World Economic Forum (WEF) in 2011.[89] The respective classification options are given in the table below.

Table 2 Classification of data according to WEF, cited by European Commission, 2019

Classification dimension	Dimensions
Data acquisition	• Volunteered: intentionally contributed by user of a product • Observed: behavioural data obtained automatically from a user or a machine activity • Inferred: obtained by transforming data of the former two types
Data use	• Non-anonymous use of individual-level data: data of type volunteered, observed or inferred, used to provide a service to an individual • Anonymous use of individual-level data: as in the bullet point above, but the data is anonymous (e.g., for machine learning) • Aggregated data: more standardised data that has been irreversibly aggregated (e.g., sales data, national statistics data) • Contextual data: Data derived not from individual data (e.g., satellite data, road network information, etc.)

Source: European Commission, 2019.

[88] European Commission, 2019.

[89] World Economic Forum (2011). *Personal Data: The Emergence of a New Asset Class*. https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

In the discussion with the scoping interview partners, the most common classification systems were the dimensions of raw vs. processed data; structured vs. unstructured data;[90] personal vs. non-personal data and machine- (sensor-)generated data[91] vs. human-generated data. There were also other classifications and types of data discussed, however.[92]

There are classification systems that attempt to categorise machine-generated data further,[93] or provide a classification of different types of industrial data, according to sources and usages of the IoT (Internet of Things).[94] The frequency by which data is collected (real-time or not) is yet another dimension that could be considered (and actually crosscuts most of the other classification systems).

Eventually, there are also industry-specific types of data, many of which have been developed because of regulatory requirements. Kerber & Gill (2019), for example, discuss repair and maintenance information (RMI) in connected cars.[95] It becomes evident that most of the definition attempts with respect to machine-generated data are linked in some way or another to the bigger topic of Internet-of-Things (IoT) in the academic literature as well as in industrial publications and blogs.

Scaria, et al.[96] used the following classification in their survey:

- Data generated by the Internet of Things (IoT) and physical devices, including sensors or mobile phones
- Data generated by internal IT business systems, mainly containing information about products, services, sales, logistics, customers, partners or suppliers (CRM, etc.)
- Data generated through external interaction with users (i.e., cookies, web tracking, logs)
- Data generated from crowdsourcing or web collaboration

[90] https://www.talend.com/resources/structured-vs-unstructured-data/, last accessed 1 May 2021

[91] Abadi, D., 'Machine vs. human generated data', 30 December 2010 available at http://dbmsmusings.blogspot.com/2010/12/machine-vs-human-generated-data.html.

[92] It was reported that major pieces of data that are being shared as confidential and commercially valuable involve files like construction designs (CAD files) or technical specification data that must be shared with other partners so as to make, for example, different parts of machines inter-operable. Hence, we included this kind of data in the questionnaire. Similarly, there were reports that know-how related to production processes (such as the right temperatures, pressures, flow rates), e.g., when producing ingredients for drugs, are also important – this is in line with the literature that suggests that (production) process innovations are more likely to be subjected to trade secret protection. Data that pertains to business information was a third category mentioned. This sort of "shared" data includes things like contract clauses, royalty rates (terms of licensing), revenue and financial data. Hence, we also included a category for "business data".

[93] Shinall, V., 'The 5 Types of Sensor Data Used by Businesses & Organisations' (2019) available at https://blog.temboo.com/5-types-of-sensor-data/. The author distinguishes between live sensor data (to monitor developments in real-time), historical sensor data (e.g., to create records for compliance purposes), analytical sensor data (to learn and assess), predictive sensor data (to forecast and plan) and "data for change" (to build consensus and make improvements)

[94] E.g., XMPro, '7 Types of Industrial IoT Data Sources (And How To Use Them)', available at https://xmpro.com/7-types-industrial-iot-data-sources/ (last accessed September 2022). The seven types are: 1. Industrial control systems (such as for predictive maintenance), 2. business applications (combining data from CRM (Customer Relationship Management), ERP (Enterprise Resource Planning) and EAM (Enterprise Asset Management), 3. Data from wearables, 4. Data from sensors, 5. Open and web data, 6. Media data, 7. Location data

[95] Kerber & Gill, 2019.

[96] European Commission, Directorate-General for Communications Networks, Content and Technology, Scaria, E., Berghmans, A., Pont, M., et al., *Study on data sharing between companies in Europe: final report*, Publications Office, 2018, available at https://data.europa.eu/doi/10.2759/354943.

3.2.2.2 Final typology used in our survey

Out of all these classification attempts, the one that was (also) discussed in interviews was that of open data/databases as a possible question of interest. In the end, a decision had to be made with respect to which type of data to include in the questionnaire for the survey (and interview guideline) given the limited space available and the need to easily convey a typology. A working hypothesis after the scoping interviews was that one of the most important typologies of data is the one related to content, particularly data incorporating know-how. The reason is that this type of data a) needs to be on many occasions shared as well as b) this may be the major type of data to which trade secret protection is directly applied. Table 3 below presents this selection for the interview guideline. A subset of these classifications, for the sake of brevity, was selected for the questionnaire (in bold).

A discussion ensued with most of the scoping interview partners with respect to the term "machine-generated" data, as many types of sensor-generated data may still be processed by humans. To overcome this issue, we introduced the term of predominantly machine-generated data. We made a further differentiation between machine-generated data in production / manufacturing (manufacturing machines collecting data, e.g., in the setting of "factory of the future"), and data coming from components of products / services in use. In one interview, contextual external data, such as satellite positioning data, weather data was mentioned. However, these are more openly available data and hence not necessarily susceptible to trade secret protection.

The scoping interviews indicated that these could be important differentiation dimensions for later policy recommendations. Similarly, there was a discussion on personal data vs. non-personal data (also a distinction often not simple to make), as well as a discussion on the overlap of sensor-generated and personal data (e.g., sensors that log access of workers / employees to certain areas in a factory).

Table 3 Ways of classifying data, as used in the interview guideline and in the questionnaire (selection for questionnaire in bold)

Possible way of classifying different kinds of data	Example
…by the way data is generated and/or aggregated	**(predominantly) machine-generated or (predominantly) human generated**
…by the way the data is structured	**Unstructured vs structured data**
…by the way data is stored before being shared	on a local electronic device; on local company server; group-wide intranet; private cloud; public cloud
…by the way data is being transferred	manual / ad-hoc vs automated (APIs, standardised);
…by use/purpose of the data	to improve performance of an existing product or service; to develop new products or services; to enable new business models, etc.
…by level of processing	**Raw data (e.g., input for AI-model training) vs. processed data (e.g., data generated by AI-models), aggregated data**
…personal data	**personal data or non-personal data**
…by content of data	**e.g., mere sets of numbers/signs or knowhow-how incorporating data (e.g., construction files/data), (production) process know-how; business data (such as contract clauses, financials); regulatory data (used because of regulatory requirements, e.g. safety data, trial data)**
…by scope	**e.g., single data points/streams vs. sets of data / databases / combined data**
…by other means…	e.g., very industry-specific types of data

Source: Study team

Further remarks were raised particularly regarding the changing significance of different types of shared data, and to differentiate between the current situation and the future situation. Regarding the future situation, it was suggested to introduce a measurable timeframe, as otherwise all types of data sharing would be in the (distant) future "significant". We decided to set the time at five years from now.

3.2.3 Scenarios of data sharing

Both literature and the scoping interviews agree that there is a plethora of scenarios foreseeable where the sharing of confidential and commercially valuable data takes place.[97] Having said that, the scoping interview partners regarded the generic types of scenarios as integrated in the scoping interview guideline as well reasoned and covering major scenarios. Only two more specific additions and adaptations were discussed: (a) a specific scenario where a company asks another for data to train an AI model; and (b) a scenario where data from different sources must be drawn upon to create value-added.

Montjoye, et al., in a European Commission report of 2019, chose three types of usage scenarios to demonstrate and make their points on competition policy matters:

Table 4 Major scenarios for data sharing as suggested by Montjoye, et al.

Nr.	Scenario
1	In scenario 1, a dominant firm has individual level data – whether personal (scenario 1a) or non-personal (scenario 1b) – about a specific person (or machine used by a person); this data is needed by another firm to provide complementary services to a product, or a service provided by the dominant firm to that specific person. For example, a firm offering a follow-up service for e-mails may require continuous access – that is access as the data is generated – to users' inboxes and calendars (scenario 1a), or a firm offering maintenance services for aircraft may desire to have continuous access to sensor data from a specific aircraft it wants to service. In scenario 1a, the data access request will typically require consent by the data subject (if the data is personal) and in scenario 1b by the machine owner or possessor.
2	In scenario 2, a firm requests access to bundled individual level data or to aggregate data from a data controller. For example, the firm offering maintenance services for aircraft is not satisfied with access to the sensor data for the aircraft which it services but wishes to also access the sensor data of all aircraft of the same type, to better predict upcoming problems. In such a setting, the firm requesting access may either offer services that are complementary to the product or service offered by the data controller (scenario 2a), or it may compete with the data controller in the downstream market (scenario 2b).
3	In scenario 3, a firm requests data from data controllers for the purpose of training algorithms for uses that are completely unrelated to the fields of activity of the data controller. As we have discussed before, large-scale datasets collected for one purpose, e.g., location data, can be valuable for a broad range of applications. Therefore, scenario 3, too, is a relevant and important scenario.

Source: European Commission, 2019.

The definitions of Montjoye, et al. are too extensive to be included in a questionnaire, however there is a high degree of correspondence with the scenarios already enquired into in the scoping interview guideline.

3.2.4 Identification of interesting potentially valuable data assets

The identification of interesting data assets proved to be a question that triggered considerable interest among our scoping interview partners and experts. It seems this issue is not sufficiently known and/or understood, while at the same time it was regarded as a question of high relevance for businesses. One interview partner said, for example, that "*…identifying the data assets that could be shared and then the means by which to commercialise them"* (interview) would be THE key activity for firms in the data economy.

[97] See European Commission, Directorate-General for Competition, Montjoye, Y., Schweitzer, H., Crémer, J., *Competition policy for the digital era*, Publications Office, 2019, available at https://data.europa.eu/doi/10.2763/407537, p. 75, where it says: "*There are myriad different circumstances in which a firm could wish to have access to data controlled by another firm.*"

Accordingly, we introduced a separate question for internal and external identification of datasets.

Certain issues and challenges faced by businesses were discussed when identifying data sets either internally (within the firm; internal side) or from outside sources / third parties (external side):

- On the internal side, most interview partners noted that one issue was that companies might frequently not be able to identify valuable confidential and commercially valuable data assets. One reason is that they might be too much pre-occupied with "traditional" means of identifying and appropriating IP assets, notably patents, which would not sufficiently cater for the large scope of protectable matter with trade secret protection. An example of how to tackle the identification of valuable confidential and commercially valuable data was given with a large Asian semiconductor firm, which has recently introduced "idea competitions" among employees, to identify potentially trade secret protectable (data) assets and ideas on how to commercialise them. The interview partner said: *"This is radical in that trade secrets are not seen as precipitating from patenting processes but have a life of their own, beyond patents."* (interview) The results of this "trade secret" challenge at the Asian company – together with the awareness-raising that has taken place for this IP-like instrument – were said to be encouraging (no further details on the outcome were given, though). Another company uses war-game-like simulations: During a workshop, a scenario is played where employees are asked to consider the case whereby they leave the firm to found a competitor. What would be the data and secret know-how they would need to (unlawfully) carry with them, from their "former" employer, to start a competing business?[98]
- On the external side, it was noted that a particular challenge is when confidential and commercially valuable data is carried over by new staff from the previous employer – i.e., the access to the confidential and commercially valuable data is unwanted. The problem is: a) in identifying such instances and b) ascertaining actions to be taken after that.[99] One company discussed in a pharmaceutical context also the danger of the company becoming "contaminated" with a foreign trade secret of a collaboration partner*: "A case in point could be an originator pharma firm, which seeks new formulations for its drugs, informs us of what they are up to and look into our databases. In such cases, we could get knowledge of data and trade secrets of the pharma firm, which we could otherwise have developed and maybe then patented on our own"* (interview partner). For respective situations, contracts may include some sort of anti-NDA clauses which stipulate that if the company gets knowledge of respectively defined trade secrets, this should be considered an act of disclosure.

3.2.5 Protection measures for confidential and commercially valuable data

All interview partners in the scoping interviews agreed that the protection measures for shared confidential and commercially valuable data was a highly important question in the context of the study, with several amendments being suggested. Chief amongst these was the observation that the scoping interview guidelines covered legal protection measures and TPMs, but did not account for business processes and the managerial aspects. This caters, in particular, for the aspect whereby the biggest source of secrecy leakages are employees who leave the company, switch to competitors or set up their own firms.

Accordingly, there would be a need to address this issue in managerial processes in three places: when staff are hired; when existing staff are trained and made aware of the issues at stake through a corresponding policy; and when respective staff are leaving the company. Hence, we included these three process steps explicitly in our questionnaire. In addition, one interview partner informed us that having a dedicated unit / department /

[98] The relationship between trade secrets and employment law is discussed further in section 5.3.

[99] This could be a form of trade secret misappropriation, but not necessarily. It depends on the data and whether it forms part of the ex-employee's know-how.

person responsible for data sharing and protecting the shared data could considerably improve the company´s capability to enact trade secret protection, too. We therefore included this as a managerial / process category.[100]

As far as trade secrets protection is concerned, some interview partners saw trade secrets as the major tool to protect confidential and commercially valuable data, while the others contemplated trade secrets to be only a smaller tool in a larger toolset, including other types of IP (sometimes database rights, copyright), TPMs, contract law. With many interviews, there was a common theme emerging, however, which is that trade secret protection for shared data (other than data whose content is know-how) has yet to be explored as a protection tool. The respective future-use cases are associated particularly with big data sets and AI-training models, where the companies indicate that they are only in rather early respective development phases. Hence, in many instances, trade secrets may currently not be very suitable for the shared data itself (data "as such", respectively raw data). There seems to be a stance that such data should be often shared openly. Trade secret protection may be correspondingly the tool of choice for the way the data is processed.[101] The exceptions to this possible "rule" are a) data which exemplifies know-how; and b) for the case where data is brought together from different actors to identify new patterns using novel methods of analysis, such as described in the pharma sector.

Surprisingly, few pieces of literature seem to have attempted to study the use of trade secrets for shared confidential and commercially valuable data. The most notable exception is the study of Prof. Drexl from the Max Planck Institute, in 2018[102], written for the consumer association BEUC. This study deals with data access and control in the era of connected devices. It discusses the various issues comprehensively, including the pros and cons for a data producer´s right (a concept which Drexl opposes) and data access rights using a FRAND approach (which the author favours). One chapter discusses the evolving legal framework of the EU for the data economy and dedicates, within this chapter, one section to trade secrets protection.

Drexl argues very positively on the use of trade secrets regarding its suitability as a protection mechanism when data is exchanged between connected devices:

> *"In contrast to the sui generis database right, EU trade secrets protection has to be considered a useful tool to improve the working of the data economy with regard to data generated by connected devices. The EU Trade Secrets Directive achieves this goal by establishing a more balanced system that allows to take the interests of other market participants, including their interest in access to data, into account. Conceptually, although the regime protects data on the semantic level, the Directive does not protect against any unauthorized use of trade secrets but only against specific forms of illegal conduct which typically requires a breach of confidentiality obligations. On the operational level, excessive protection of data protection is avoided in various regards, namely, as regards the definition of trade secrets, the scope of protection and, finally, the remedies. In particular, the judge is given broad discretion to decide cases flexibly in the light of fairness considerations. Protection of trade secrets against third persons that are not directly bound by confidentiality obligations goes very*

[100] The relationship between trade secrets and employment law is discussed further in section 5.3.

[101] To give an example of a use case: For monitoring a machine in use, sensor-generated data could be shared rather openly as raw data (the data that is directly generated by the sensors) and hereafter also as processed data (after a software analytics tool has processed the data) – there may not be too much value in the data "as such" (because it is more beneficial to share it and/or because it would be difficult to protect it). The true secret rests in the way the data is processed, i.e. the algorithms on how to process the data which stays or should stay secret. The issue of raw data vs. processed data and its susceptibility to trade secret protection is discussed further in section 5.2.1.

[102] Drexl, 2018.

> *far, but this is still acceptable in the light of the knowledge requirements for liability."*[103]

For Drexl, the most obvious beneficiaries of trade secrets are manufacturers of connected devices, who would enjoy a second layer of protection to the de facto existing flexibility. Furthermore, manufacturers of said devices will particularly benefit if they *"…aggregate data on the functioning of all connected devices in order to further improve and develop these devices. Moreover, specific categories of data may also be aggregated in an anonymised form to commercialise these data in secondary markets. For such purposes the manufacturer will also need to keep the information contained in these datasets secret to be able to charge a price for granting access to the information contained in the data."*[104]

However, commercial customers of said manufacturers would also benefit if they impose confidentiality obligations on the manufacturer. For example, an operator of a factory could limit data transfer from the manufacturer of a machine used for production to a third party, if it would hereby breach trade secrets of the factory operator. By contrast, Drexl does not think that trade secrets are relevant for the use case where the intention is to share data on large data sharing platforms: *"Trade secrets protection will also not be needed and, hence, fail to come into existence when the data produced by connected devices will be exchanged on large data sharing platforms, for instance, to enable automated or autonomous driving."*

3.2.6 The impact of the Trade Secrets Directive and the relationship with contract law – a first glance[105]

Our interview with a representative from a large manufacturer of machines used in factories – i.e., exactly the type of company Drexl believes to be benefitting most – reported that following the enactment of the TSD, the company changed its business practices insofar as it implemented a range of measures to account for the requirements that must be met to meet the definition of a trade secret. It trained its staff; it introduced policies by which employees would need to classify information as for the public, for internal use only, confidential information to be seen only by select persons in the company; and to act accordingly. Complementary measures included actions taken to improve IT-security.

The interview partner told us that the new practices, in terms of basic substance and as far as they presented themselves to outside parties, were the same as before, where the respective confidentiality matters were handled (mostly / only) in contracts. The major difference to the previous practices, resulting from the TSD, lies in an expected improved enforceability. However, to date the company has not yet had litigation or enforcement action in this regard, and is also not aware of any landmark decisions, so whether the Directive delivers on the expectations is a matter that needs to be seen.

Another company – which also stated that it handled trade secret protection via contracts and who we questioned regarding the specific benefits of the TSD on top of these contracts – reported impacts of the TSD in terms of managerial practices. The reason lies in the specifics of trade secret protection *"…which do not come with well-defined deadlines and hence, there is less of a sense of urgency compared to, e.g., patents."* In addition, as trade secrets in the past were covered in different parts of the (national) law, so were different aspects of trade secret protection handled by different departments; i.e., the legal department, the IP department, the IT department and/or corporate security. Trade secret protection also comes with costs, which are associated with implementing the "reasonable steps" to maintain secrecy. Taken all together, a situation ensued in the past where nobody felt truly responsible for trade secrets, the topic was felt as cumbersome, expensive, and

[103] Drexl, 2018, p. 11.

[104] Drexl, 2018, p. 94.

[105] The relationship between trade secrets and contract law is further assessed in section 5.4.

not urgent (compared to other day-to-day duties), so it was put at the end of the agenda. For our interview partner, the TSD had a significant impact in that it unified and standardised the topic to an extent and created the sense of urgency needed. Therefore, trade secrets now have also a clear institutional ownership (in the IP department).

These issues prompted us also to look from a legal angle at the relationship between contract law and trade secret law, to better understand in detail the benefits of having an additional trade secret over a "simple" contract.

3.2.7 The different grey shades of trade secrets – and societal vs. private concerns

Another consequence stemming from the interviews is that there may be different levels of confidential and commercially valuable data, depending on the value of this data for the firm.[106] Within our team, we also discussed that increasing value of confidential and commercially valuable data translates also into a need for stronger protection measures – so to ask about the adequacy of protection measures in the questionnaire should be framed against the risks of loss of value and the respective impacts associated with misappropriation of trade secrets. This speaks to both Arrow's paradox, in that companies must understand the costs and benefits of sharing, but also of the practical challenges in determining efficient levels of protection.[107]

Hence, there is also the phenomenon whereby, in practice, there may be different qualities or levels of trade secrets – from "not so important, nice to have" trade secrets to "crown jewels", where it would really hurt losing them and where there need to be severe protection measures in place. Academic literature supports this distribution – while some trade secrets are incredibly valuable, most are not.[108]

The wider environment in which trade secrets operate adds nuance to their function. Trade secrets have often been framed as providing a weak outcome for economies, as their secrecy restricts the flow on knowledge, leading to poorer outcomes for social welfare.[109] Yet trade secrets can be welfare enhancing. For example, as trade secrets can be licensed, they may promote innovation, more so than patents in markets for complex markets, as a study by Ottoz & Cugno suggests.[110] The authors argue that trade secret licensing fosters a long-term oligopoly, whereas patents construct temporary monopolies which are followed by perfect competition; social welfare is higher under the oligopoly. We cannot, therefore, conclude that trade secrets are necessarily welfare damaging.

3.2.8 Modes and conditions for data sharing

Scoping interview evidence with respect to the modes of how data is shared (mostly contract terms and governance modes) was positive, insofar as the dimensions of the scoping interview guidelines were clear to them and relevant. However, combining the

[106] This issue is also further discussed in section 5.2.2.

[107] E.g., Gordon & Loeb, 2002.

[108] Reid, G.C., Searle, N. & Vishnubhakat, S., 'What's It Worth to Keep a Secret' (2014) 13 Duke L. & Tech. Rev. 116.

[109] Denicolo, V., & Alberto Franzoni, L., 'Patents, Secrets, and the First-Inventor Defense' (2004) 13(3) Journal of Economics Management Strategy 517–538, available at https://doi.org/10.1111/j.1430-9134.2004.00021.x; Panagopoulos, A. & Park, I., 'Patents As Negotiating Assets: Patenting Versus Secrecy For Startups' (2018) 128 The Economic Journal 2876–2894, available at https://doi.org/10.1111/ecoj.12540.

[110] Ottoz, E. & Cugno, F., 'Patent-Secret Mix in Complex Product Firms' (2008) 10(1) American Law and Economics Review 142-158.

literature and interview evidence, we found that there could be many more additional dimensions added.

3.2.9 International dimension

In terms of international dimensions, an issue that was raised in the interviews was that of export control mechanisms. For firms, export control regulations prompt an additional layer of scrutiny, as confidential and commercially valuable data and respective trade secrets must also be examined as to whether they would/could fall under export control mechanisms and be banned from sharing with certain countries, like Russia or China. However, though to a much lesser extent, this was said to also be of concern when sharing confidential and commercially valuable data / trade secrets also within the EU across borders (from a subsidiary in one country to another country – although no further details are available on how this problem manifests itself in practice).

4 Confidential and commercially valuable data sharing and trade secrets – empirical results

4.1 Collection and use of confidential and commercially valuable data – data sharing practices

Backed by the literature review and the scoping interviews, we created an improved interview guideline and a web survey to collect empirical evidence. We start our section on empirical results by looking at data sharing practices in this section 4.1. We hereby provide an overview of whether and which types of confidential and commercially valuable data are shared under different circumstances. We use the survey, interviews, and case studies as sources of evidence. In order to increase readability, we outline the major findings at the beginning of each (three-digit hierarchy level) section.

To note: Some analyses, particularly a number of those breaking up results into sub-groups such as different sectors, pertain to a low number of responses (low number of n). Hence, statistical significance is hardly given. We decided, nonetheless, to report these figures for indicative purposes and took account of this issue, e.g., by quoting absolute values more often than/instead of percentages. Readers are advised of this issue and to take proper care when interpreting the results.

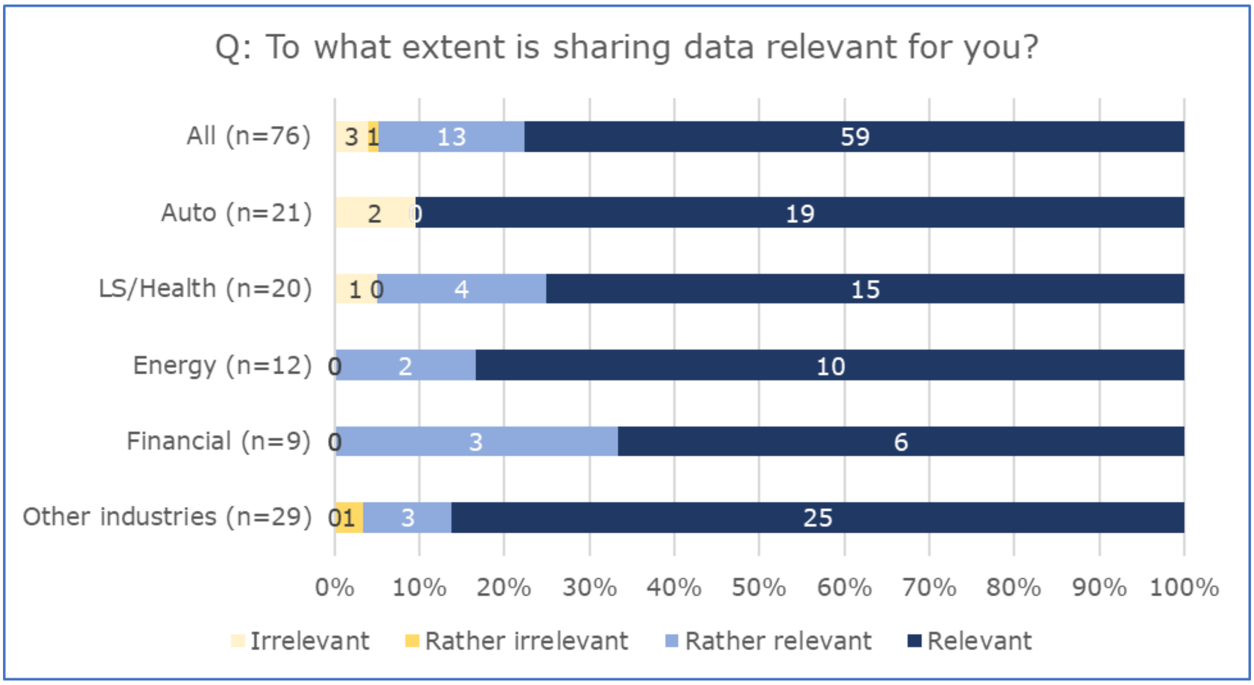
4.1.1 Significance of data and confidential and commercially valuable data sharing

Major take-aways

- Data sharing is relevant for the interviewed and surveyed firms
- Its significance will increase further in the future
- The energy and financial industries seem to trail behind the other sectors inquired into when it comes to data sharing

Figure 4 shows the significance of data sharing for the respondents as delivered through the survey. As can be expected, most respondents deemed the subject matter as relevant. Only a few believed that data sharing is "rather relevant" and very few stated the subject matter to be "rather irrelevant" or "irrelevant". This seems to be true irrespective of the industry that we looked at.

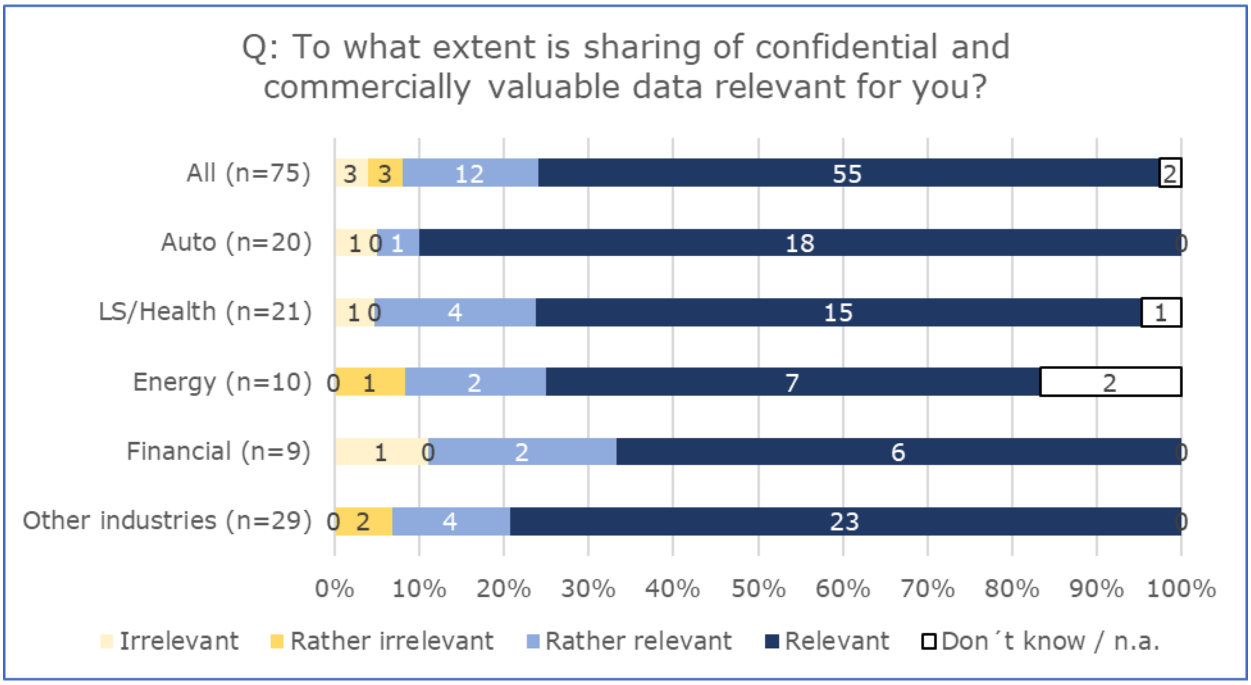
Figure 4 General significance of sharing of data



Source: Survey

A similar picture emerges if we look only at the importance given to the sharing of commercially valuable and confidential data (see Figure 5). However, we can also observe subtle differences. Whereas the majority of respondents again deem the sharing of confidential and commercially valuable data to be relevant, this opinion seems to be more pronounced in the automotive industry, in the life sciences and health industries as well as in the “other” category, but less so with the respondents in energy and financial services – which basically echoes interview evidence that, for the latter two industries, confidential and commercially valuable data sharing is, to a degree, more of a future topic, a *“…future that is in the making”* (interview partner in the energy sector).

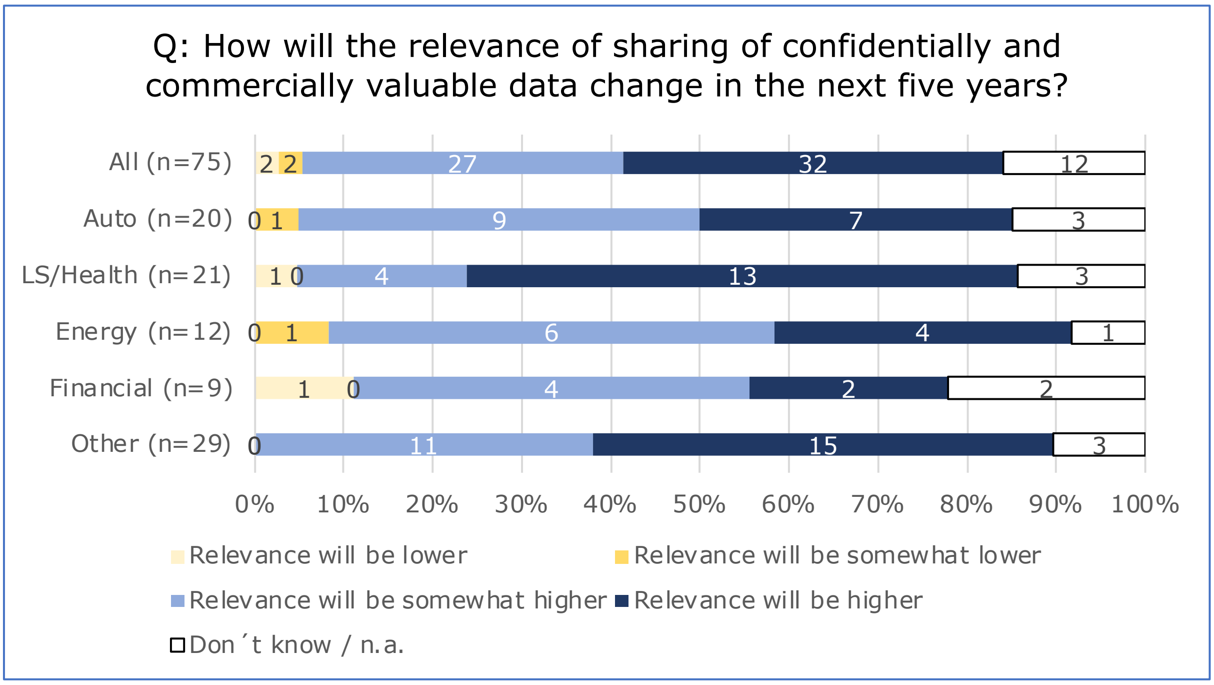
Figure 5 Significance of sharing of confidential and commercially valuable data



Source: Survey

For the foreseeable future (i.e., the next five years), survey respondents expect a "rather increasing" or "increasing" relevance of sharing of confidential and commercially valuable data (see Figure 6). This situation can be observed across all sectors. However, of note is also that a non-negligible share of respondents is not sure about the future direction.

Figure 6 Future relevance of sharing of confidential and commercially valuable data



Source: Survey

Considering interview evidence, we observe that, for many companies, the journey of data sharing and using trade secrets has just begun, particularly also in the energy sector. Case Study Nr. 1 below illustrates this.

Case Study Nr. 1 – Energy utility firm and its beginning journey into confidential and commercially valuable data sharing and trade secret usage

Sector:	Utilities (energy)
Type of organisation:	Large firm
Type of data shared:	Various
Data shared with:	Service providers, collaboration partners
Use of trade secrets:	yes

The company in this case study is a leading energy utilities firm in a small EU Member State, selling electrical energy, natural gas, and district heating. While the company attaches great importance to the current sharing of data, the importance is even greater in the foreseeable future due to increasing digital transformation and technical facilitation. They acknowledge that the requirements from the business sector for the shared use of data are increasing, as are the platforms and projects that have precisely this goal. Projects themselves are largely in the pilot phase to gain experience with this topic. A special focus is being put on data governance to be able to deal with clear specifications and terms. In the past, the company has gained experience, especially within the framework of cooperation agreements, consulting contracts, as well as services/ contract processing for operative business areas and IT, purchasing, services, sales, and distribution.

Data is shared with companies within the group, service providers (within and outside the group) as well as collaboration partners. Data is shared first and foremost to handle business operations professionally, appropriately, and efficiently. The scenarios of data sharing take place in all business areas at almost all levels, depending on the needs of business operations within the framework of specialisations based on the division of labour, within the framework of cooperation agreements or service agreements, considering appropriate competition, strategy, and confidentiality considerations. Other reasons include contract fulfilment, product development and location assessments. Against this backdrop, data that could potentially be shared includes machine data (e.g., sensor-generated energy data, metering data), data from cloud storage, personal data (e.g., consumption behaviour, billing data), industry specific data (e.g., effects of technology in terms of temperature, efficiency), marketing data (often public data, such as prices, but also forecasts), asset data. Barriers for not sharing data include concerns that the competition could gain a competitive advantage through knowledge of one's own trade secrets. These barriers can also be differentiated according to the degree of secrecy: reasons of competition, strategy, no sufficient level of data protection in technical or legal terms.

The prevailing view is that the protection of shared data can only function organisationally by means of a set of rules from a legal and organisational perspective, which is then implemented technically. The company uses the instrument of trade secrets from the perspective of information security. The EU Directive 2016/943 was implemented by reviewing and revising/adding to contracts and clauses (sales, purchasing, personnel), NDAs, confidentiality notices, corporate guidelines. Further discussion of this matter takes place together with the data protection and legal departments, if necessary.

In summary, it can be stated that the handling of confidential and commercially valuable data will certainly gain in importance soon, as additional insights can often be gained by aggregating a wide variety of data. It is important to have internal rules so that everyone involved is aware of how to deal with such data and the special sensitivity of this topic. With the inevitably extensive (and, in the future, foreseeably even greater) use of large IT service providers and cloud providers, it is not always possible to check whether they are not using the data for their own or other purposes or disclosing it to authorities for whatever reason; under this aspect, the protection of confidential and commercially valuable data is only a relative one.

This is not assessable regarding the protection of patents, copyright, database rights and other IP rights for the companies concerned, nor can it be shaped by contracts (even for large companies). Due to increasing digitalisation and the further development of technical possibilities, this topic will gain in importance; it will therefore become increasingly important to create the appropriate legal and technical framework conditions.

Additional evidence is given by the following interviews:

- Interviews with two SME energy supply companies confirm the prevailing view described in the case study above to a large extent. However, both companies currently rely on NDAs and put trust into their cooperation with customers and suppliers. Trade secrets are currently only used to a limited extent or not at all. Both companies plan to discuss trade secrets in detail and implement them in the future in their companies.

- An interview with an energy company also confirms the above statements. This firm has already established a programme and a policy managing trade secrets, assuring proper legal, organisational, and technical measures in their organisation. In this regard, a trade secret governance has been established identifying roles, processes, and responsibilities. According to the firm, trade secrets are a proper measure to protect confidential and commercially valuable data and will be shared in the future and need to be treated with a high demand of confidentiality and privacy.

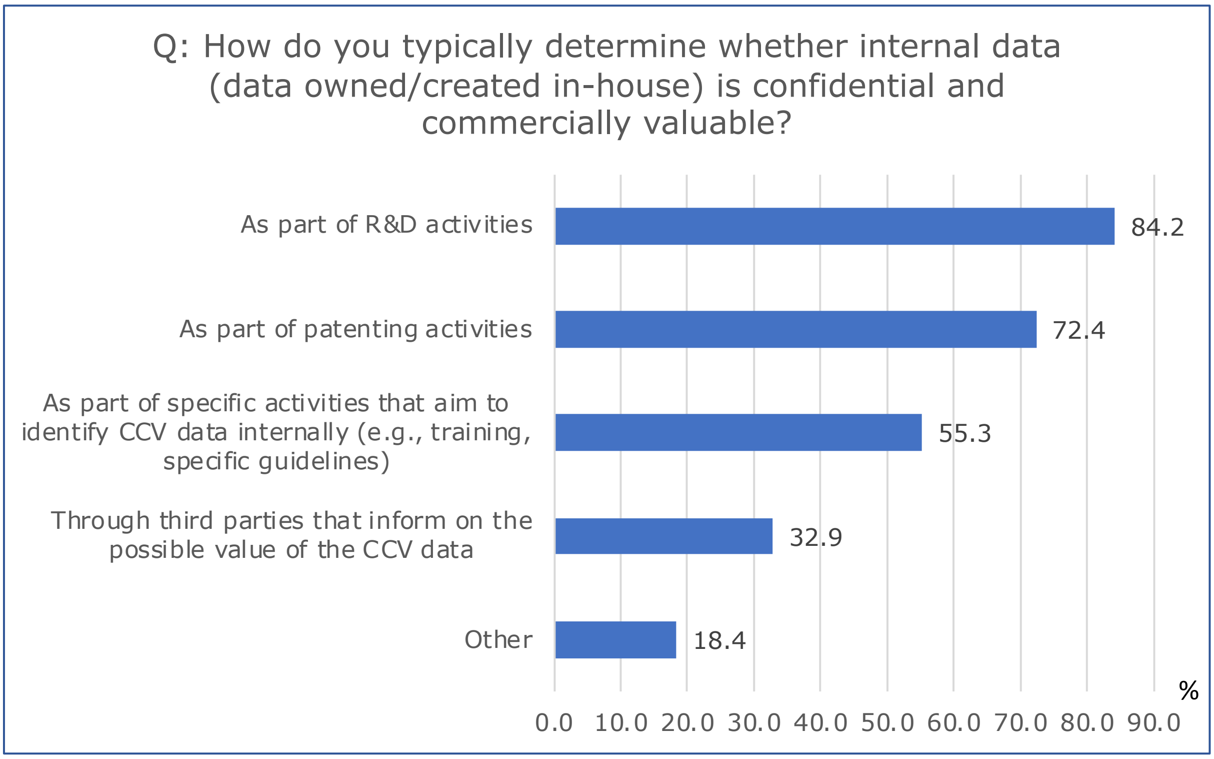
4.1.2 Identification of sources for confidential and commercially valuable data

Major take-aways

- The most important internal sources to identify sharable confidential and commercially valuable data is from R&D, followed by patenting activities
- Identifying data needs and hereafter third parties having this data is the most important way of identifying data from other/external sources

We now turn our attention to how our respondents source their confidential and commercially valuable data. Figure 7 provides the answers for company-internal sources of confidential and commercially valuable data. A clear ranking becomes visible: some 84% harvest confidential and commercially valuable data as part of R&D activities; 72% also as part of patenting activities. 55% operate specific activities that aim to identify data sources – this relates to training, specific guidelines. Some 33% are alerted by third parties on the possible value of the data (for us, quite a high share, which indicates that more than a third of the firms may sit on data treasures and do not fully realise that, without information from outside). Other, diverse, internal sources play a lower role.

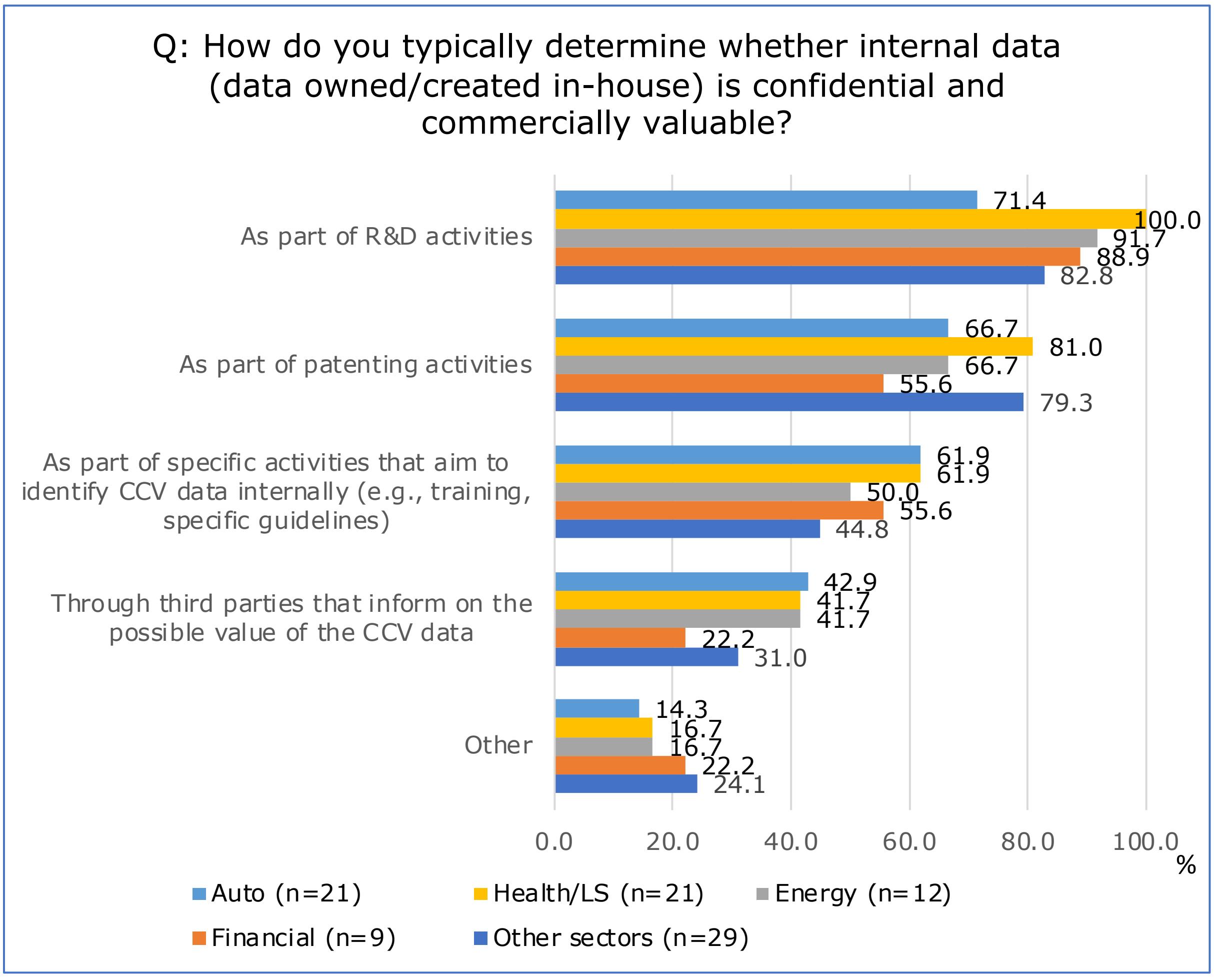
Figure 7 Internal ways to determine whether data is commercially valuable and confidential, shares of firms answering *)



*) multiple responses possible
Source: Survey, n=76

A sectoral breakdown for company-internal confidential and commercially valuable data sources is provided in Figure 8. One can observe that in the health-and life sciences, data is heavily research related.

Figure 8 Internal origins of shared confidential and commercially valuable data, shares of firms answering, by industry *)



*) multiple responses possible
Source: Survey

That R&D projects and data are frequently a source for internal confidential and commercially valuable data is also illustrated in a case study (see Case Study Nr. 2 below). Also, in the "other sectors" category, we find large shares for R&D-related and patenting-related sources (and less so for other internal sources). Third parties as sources seem to be somewhat more prevalent in automotive, LS and energy sectors – for the automotive and energy sectors probably due to the evolving technology fields, which sees not only new types of data, but also new business models develop.

Case Study Nr. 2 – A health business company where data is currently mostly shared in the scope of R&D projects

Sector:	Health
Type of organisation:	Large firm
Type of data shared:	R&D data
Data shared with:	research partners, universities, research organisations, customers and funding agencies
Use of trade secrets:	Yes (but rarely)

The company for this case study is part of the health business. The firm is generally sharing some of its confidential and commercially valuable data within EU-projects – which is mostly R&D related data. Important to remark is that open access is pushed. This means exchanging mostly data which is not seen to be confidential by the firm. Within collaborative research projects confidential and commercially valuable data as well as public data is shared, i.e., data which is not confidential for the firm.

Confidential and commercially valuable data and public data will be shared with and received from research partners, universities, research organisations, customers, and funding agencies. No data sharing with direct competitors takes place. Officially the confidential and commercially valuable data exchange will only happen when an NDA or a contract with a confidentiality clause is in place. However, unofficially, some projects are only based on trust which the firm sees as a viable way to proceed under certain circumstances. By default, all internally produced data is regarded as confidential by the firm. The company has an approval process for all scientific and personal data in place.

The application of trade secrets for protecting confidential and commercially valuable data is seen as *"good behaviour"*. (interview). Trade secrets are, however, currently applied rather rarely when sharing. The mission in tech transfer is to *"pass on data with no trade secret declaration".* (interview) This implies passing on mostly data which is public and not confidential. The employees and business partners, in turn, do not need to keep data confidential, and the data sharing will be easy among all project partners. The firm is using patent protection as early as possible and thereby "protects" some of its valuable data and assets, which is seen as the best way to protect innovation and to earn money.

The major take-away from this case is that, when a firm is using the contractual protection with declared confidentiality clauses, combined with formal IP protection, trade secrets may not be as important for the business for data sharing.

The case study above also represents firms which rarely apply trade secrets. Additional evidence along this line is given by the following interviews:

- One other company interviewed from the health business is also working very rarely with trade secrets because the identification of highly confidential data is extremely difficult. Data classified as "absolutely confidential" is only data to get ahead of the competitors. The firm runs a key-process for classifying data as confidential/non-confidential and for carefully evaluating who will have access. As soon as business opportunities are recognised, the company aims to apply for a patent.
- A second healthcare company interviewed is protecting important data with NDAs and contracts with confidentiality clauses. They have confidential data, but they are not working actively with trade secrets. According to the company, trade secrets are a *"contradiction"* (interview) to patents. This firm also tries to come up with patent protection as soon as possible.

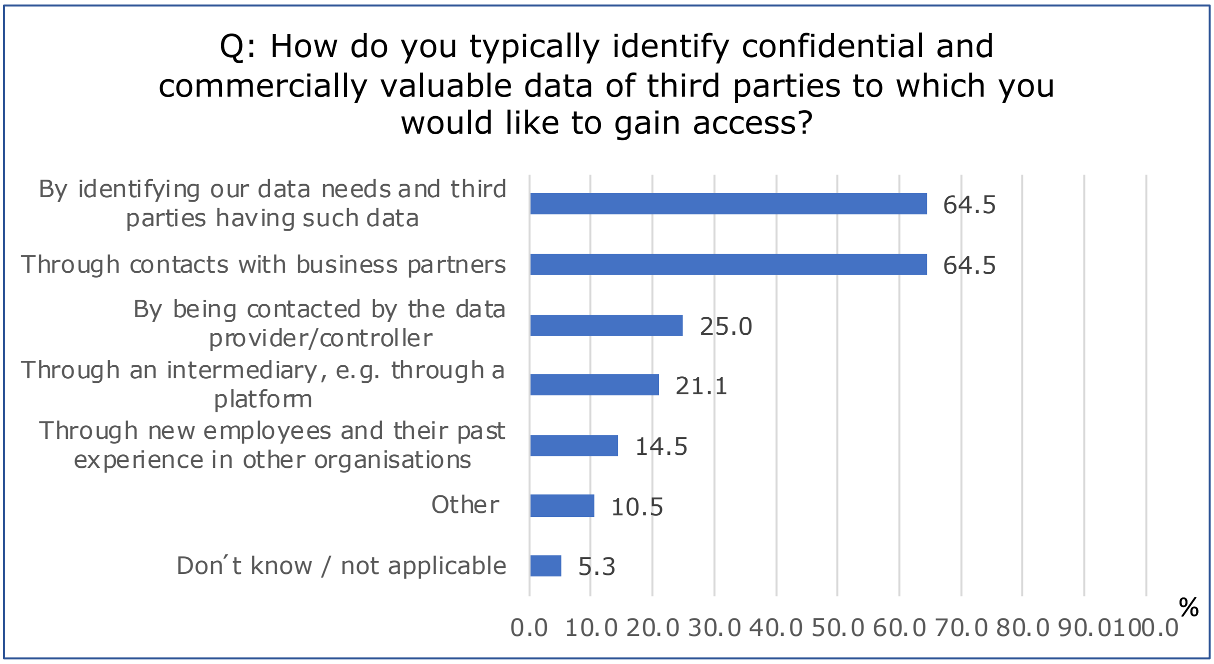
We came across, however, two healthcare firms which are mainly collecting health data and which use trade secrets (and not formal IP protection):

- The first such company collects, maintains, organises, and manages health data. They only share the data under an open license agreement comparable to open-source-licenses. In contrast to the companies mentioned above, the data sets are kept secret and protected as trade secrets and are not protected as part of patents.
- The second such firm, also working with health data, sees trade secrets as important for their business as being part of big data consortiums. Trade secrets are an important tool, both as a legal basis for contractual data sharing arrangements and as a fall-back, in case of data misappropriation and misuse. This company is also not using patent protection.

Generally, one can observe from the interviews that, for those firms where patent protection is a preferred protection mode, the data is meant to be related to (potentially patentable) know-how and/or patentable technologies of which the data is part of. Hence, the sharing of confidential and commercially valuable data "as such" is less in their focus.

Figure 9 now shows different ways the confidential and commercially valuable data of third parties is identified by our survey respondents. Two channels stand out: identifying one´s own needs and hereafter identifying third parties having such data; and through business contacts. This means that the initiative is mostly on the side of the "recipient" end for data sharing – by contrast, intermediaries, being pro-actively contacted by third parties or new employees seem to play less of a role.

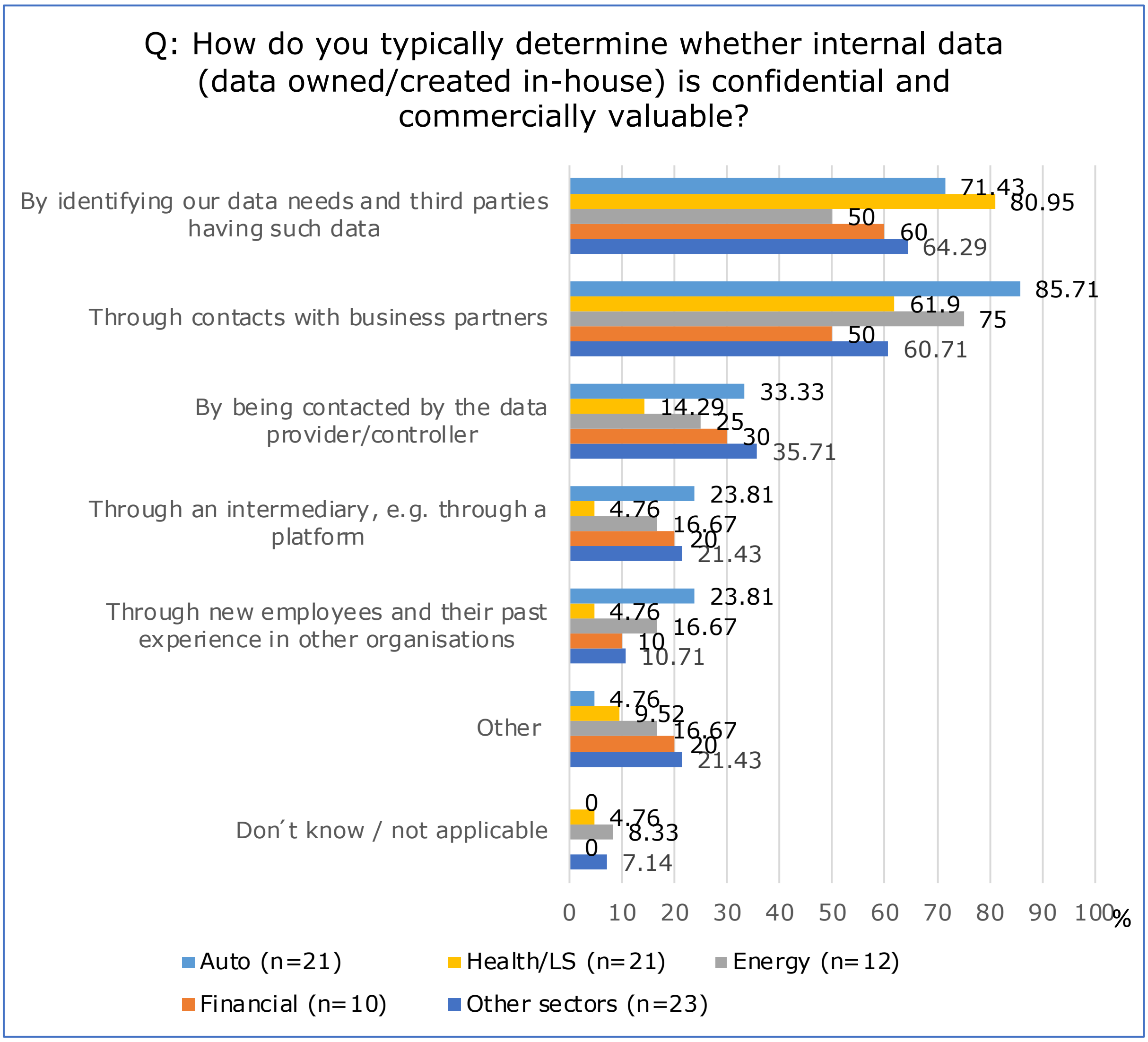
Figure 9 Ways to identify confidential and commercially valuable data of third parties to which the company would want to get access, shares of firms answering *)



*) multiple responses possible
Source: Survey, n=76

A sectoral break-down for the sourcing of external confidential and commercially valuable data sources shows differences across industries (see Figure 10). For example, firms in health/life sciences seem particularly drawn to pro-actively identifying third parties and have less inclination to use platforms and intermediaries. Firms in the automotive industry rely mostly on business contacts, probably due to the extensive supply/value creation networks prevalent in this industry. Interestingly, they are also the industry that makes the most use of intermediaries, and where contacting by third parties (data providers/controllers) takes place more often, in comparison to the other three focal sectors.

Figure 10 Ways to identify confidential and commercially valuable data of third parties to which the company would want to get access, shares of firms answering, by industry *)



Source: Survey

4.1.3 Relevance of different types of shared confidential and commercially valuable data

Major take-aways

- It is difficult to identify clear patterns of relevance regarding the types of data to be shared
- Context-specific analysis is therefore a must
- Nonetheless, it becomes evident that "classic" data and information susceptible to trade secret protection (such as know-how incorporated into data) is currently somewhat more of a use case for data sharing than the sharing of "novel" types of data

It proves difficult to identify clear patterns of data sharing in the survey according to type of data shared. This is partly also due to the fact that – despite all efforts to find suitable classification systems – in the end, one must look exactly at the type of data that is shared by a company to understand a) its nature; and b) the arising implications that arise as regards protection and appropriation regimes (see also below Case Study Nr. 3 for an example of very specific types of data in the automotive supply chain, and how this leads to specific treatment of the sharing).

Case Study Nr. 3 – OEM automotive supplier illustrating the many different types of confidential and commercially valuable data shared and arguing

Sector:	Automotive supplier
Type of organisation:	Large firm
Type of data shared:	Contracts, production-related data, training data sets for AI
Data shared with:	Research partners, universities, research organisations, customers and funding agencies
Use of trade secrets:	Yes (but rarely)

Generally, the motives for automotive suppliers (like the one in this case study) to share confidential and commercially valuable data is by demand of OEMs, e.g., for quality management and legal/liability purposes as well as for potential future business models based on data.

For automotive suppliers there are in general the following typical cases for sharing confidential and commercially valuable data:

- M&A-activities (buying/selling) and the related necessary exchange of data (contracts, often according to U.S. or UK law).
- By demand of OEMs (contractual topic). There is demand for the exchange of data on production, per single product (e.g., technical data/parameters such as on pressure, temperature, etc.), e.g., for liability purposes. The supplier is, however, hesitant to provide this kind of data as this is considered core know-how that is not supposed to be shared. Such data should only be used internally, e.g., for quality management, predictive management.
- Training data sets from the company for AI based systems (especially in R&D, production, sales). This is considered a unique selling point (USP) and core know-how for future business models, for areas like predictive maintenance, digital twin.

Data of case types two and three is treated as trade secrets and is often not shared (if not negotiated otherwise with OEMs). If it is shared with the OEM, the data is not considered as a trade secret anymore (although covered by NDAs; an NDA alone is NOT considered as appropriate means to cover a trade secret if/once shared). The tier1 supplier is, in this context, always depending on the purchase and bargaining power of OEMs.

Typical situations for automotive suppliers to share their confidential and commercially valuable data are:

- OEMs target data as a priority and try to secure access to data (of suppliers and supplied parts and systems). However, this happens, for the moment, without the OEM fully knowing the later/future use and applications of the related data. It is more a preparation for future business models (a unilateral approach from the side of the OEM).
- Data from operations (e.g., from a component in a car) is sought. So far there has been no (bilaterally) shared data for the benefit of the 1st-tier supplier (due to lack of interest or opposing interests of the OEMs). As an example, the additional use of cam sensor-based data from car operations is solely managed by OEMs and not shared with the 1st-tier supplier, even if the supplier might be able to provide additional value or improved/novel business models.

Concerning breaches and the afterlife of shared confidential and commercially valuable data, the company reported that. if data must be shared, e.g., with OEMs, the data is not considered, as stated before, a trade secret anymore. Knowledge of data afterlife use, e.g., which takes place at/with OEMs, is very limited or even non-existing. Other issues which the firm thinks need to be considered include the link between the different data sets and the various contracts (which are mainly internal challenges); and the notion that contractual parties should decide on availability, sharing and use of data by themselves, rather than being obliged to share.

In addition to the case study above, additional interview evidence for the automotive sectors suggests the following:

- This fact seems to be very important: that competition does not take place at the level of data availability, but at the level of data processing, the extraction of insights and the creation of value. Trade secrets include data generated during the manufacture of products/components, in particular data on the manufacturing process, which cannot be derived from the final product as such. This data is very valuable for the manufacturer, but not for third parties.

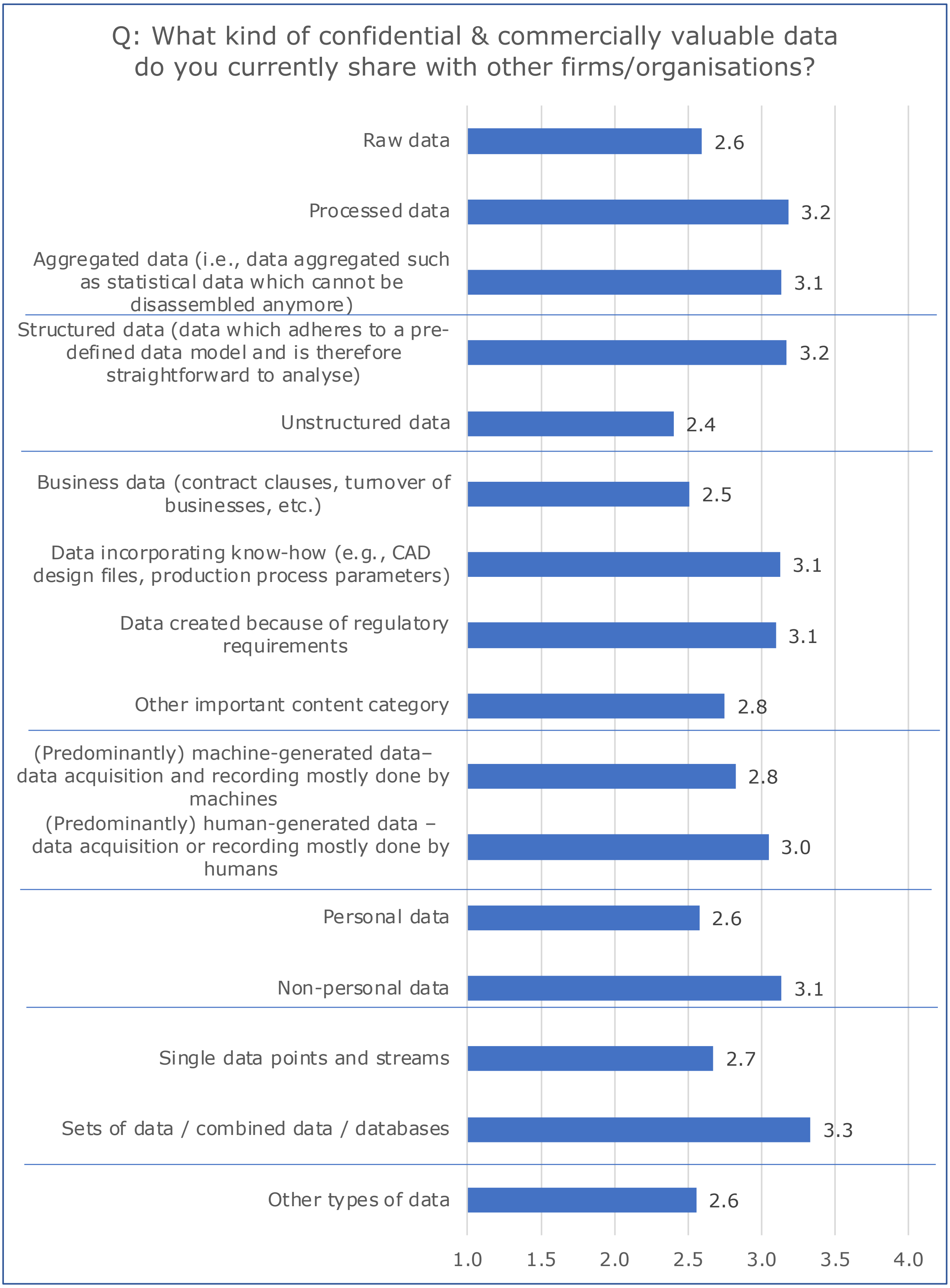
- Confidential and commercially valuable is also data collected during the use of a product/component. The data is public to some extent, but not necessarily available to the public. One interviewed firm proposed to distinguish the data according to the generation of the data, the collection of the data, and the use of the data.

Despite of the difficulties to identifying clear-cut data sharing modes, some patterns (in the sense of trends) become visible also in the survey (see Figure 11):

- Processed data and aggregated data are somewhat of more relevance in confidential and commercially valuable data sharing than raw data (in line with the interview evidence presented above).
- Structured data seems currently also more relevant than unstructured data.
- Looking at the classification according to content, data incorporating know-how as well as data created due to regulatory requirements are likely of more importance than business data, such as contract clauses, turnover of business, etc.
- Predominantly human-generated data is, in our sample, slightly more important than machine- and sensor-generated data.
- Non-personal data is, in our sample, slightly more important than personal data in confidential and commercially valuable data sharing.
- Clearly, data sets and streams are more important than single data points.

Overall, the picture emanating from Figure 11 is broadly in line with the interview evidence in that it suggests that “classic” data and information susceptible to trade secret protection (such as know-how incorporated in data) is currently somewhat more relevant for confidential and commercially valuable data sharing than the sharing of novel types of data such as the sharing of sensor-generated data. Breakdowns by sector are provided in annex A of this report. The general picture, as displayed in the list of bullet points above, is also visible in the different sectors, with variation mostly only in the extent of the differences in relevance of different data types.

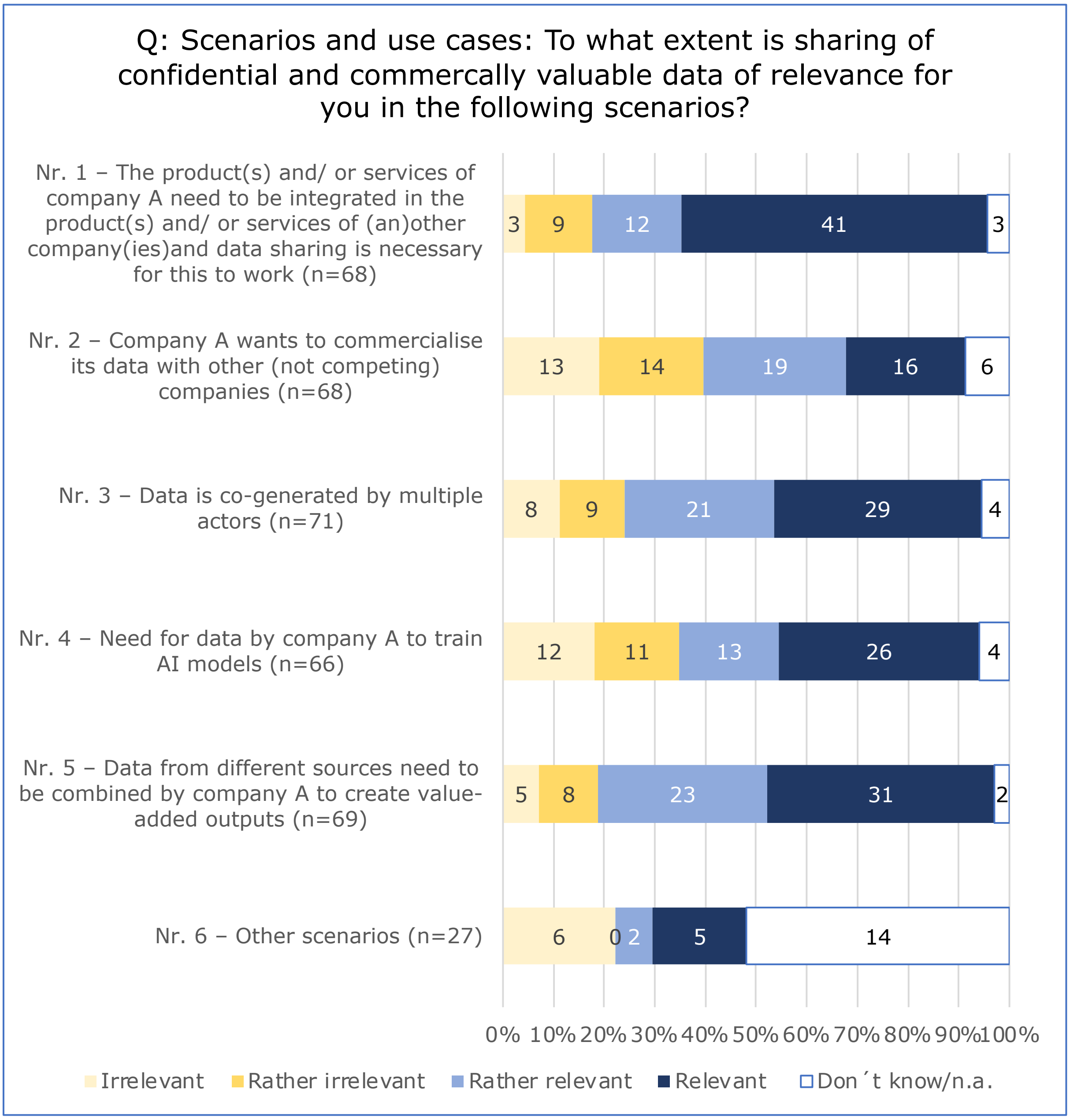
Figure 11 Relevance of shared confidential and commercially valuable data *)



*) arithmetic means of answers on a scale from 1=irrelevant to 4= relevant
Source: Survey, n=60-67 (except "Other types of data", where n=9; "other important content category", where n=16)

Eventually, we also scrutinised several scenarios of interest for the sharing of confidential and commercially valuable data (scenarios meaning different organisational set-ups) and their prevalence / relevance for our respondents. The respective results are shown in Figure 12. It becomes evident that scenario one – where a product/service of a company A needs to be integrated in a product/service of a company B, and data sharing is necessary for this to happen – is the most relevant one in our survey sample.

Figure 12 Relevance of different scenarios of data sharing, respondents in absolute numbers



Source: Survey

This is followed by scenarios five (data from different sources need to be combined by company A to create value-added outputs) and three (data is co-generated by multiple actors). Interview evidence suggests, across all sectors, that scenarios three and five are also on the rise, while scenario four (the training of AI models) is often seen as a future perspective – this is discussed, amongst others, in Case Study Nr. 4 below.

Case Study Nr. 4 – Pharma firm and its need to combine forces and share data with others so that novel treatments can be created

Sector:	Health / Pharma
Type of organisation:	Large firm
Type of data shared:	clinical trial data, molecular data, manufacturing data
Data shared with:	research partners, competitors
Use of trade secrets:	Yes

The firm in this case study is a large pharma firm.

In terms of data of interest for sharing, the company looks at all kinds of data. The data is obtained through research and commercial activities and is needed for the firm to be (more) innovative. To that end, there is a need to engage also with patients and health care providers. The major tool of protection is trade secrets implemented via contracts. There is considerable potential for data sharing and at the same time there is also a lot of value in the data and at stake. A crucial question is how the firm can fulfil the obligations to society while protecting the legitimate value of the data for the company.

The data focussed on is health-related data: clinical trial data (obtained in an "artificial" set up); real-world data (outside of the "artificial" set-up); molecular data (in the broadest interpretation: exchanged data on compounds / from combo studies); manufacturing data (when data with partners from manufacturing is shared). This data is clearly confidential and/or even highly confidential. There is therefore a considerable number of data domains. The challenge is to harmonise the data and transfer/share it in secure ways (e.g., with a third party). In doing so, there is also the need to cater for the interest of the third parties (with research partners, for example, their need to publish results; there are hence also timing issues to be resolved (when one is allowed to publish)).

Peculiarities arise in relation to the development of new compounds and new analytical tools. When the company starts to develop a new compound, there is the need to collect data on the physical characteristics. There are assays to characterise the physical properties, but these need to be harmonised and calibrated, so that the assays are reliable. To achieve this efficiently with huge amounts of data this requires machine learning and AI, which is a new trend, and these methods also need large amounts of data so that they are trained. There is therefore a need to mine datasets brought by many partners, and this is only possible through the sharing of data. Using these new AI/ML tools makes the company more efficient, and hence "data is gold".

There is, therefore, also a need to gain access to data also from third parties for the new tools. For this, there is a need to have a safe environment where the company can safely share its data without disclosing its compounds and know-how. At the moment, the systems of data sharing do work, but it is highly important that data sharing remains voluntary.

Examples of data sharing practices include the following:

- First, the company shares pre-clinical data and clinical trial data. This data is stored on the company´s own platform. The access is provided to the data via an agreement for specific purposes.
- Another example is through IMI initiatives where the initiative brings different firms and universities together to produce tools, and where the company contributes with data. Based on the data, new algorithms and tools are developed that serve the whole industry. The data sharing is voluntary for this specific purpose.
- There are also instances of bilateral agreements with data providers.
- One specific area of application is predictive algorithms for the properties of the compounds which speeds up development time and may reduce the need for animal testing. A research organisation, for example, attempts to develop a tool to predict the expected survival time of transplanted organs. To this end, there is a need to mine / re-use different sets of (already performed) clinical trial data created by different firms over time.
- Another example is platform studies where there is co-development taking place with regulatory authorities (FDA/EMA) on different arms of the platform. For example, in cancer treatment R&D, a patient might not respond well to one treatment but could possibly respond well to others. In such a case, data sharing is agreed with the FDA/EMA directly – the patient could switch from one treatment option to a more appropriate one, and the data is shared among the participants. This speeds up drug development, and there is an all-in-one solution from the point of view of patients.

The given examples and practices are mostly "one-off" agreements for specific data and specific purposes. One future scenario could be in very open platforms where data sharing for a pool of data is continuous with no specific purpose defined in advance. This scenario is highly problematic, however, because there may be no negative repercussions for parties misappropriating the data, particularly in unforeseen ways, where the company eventually also loses control over its own data.

A sectorial break-down of the scenarios by industries reveals that it is particularly the automotive sector and the "other industries" that drive the high relevance of scenario one. By contrast, the financial industry tends to place, in general, less relevance on all data sharing scenarios than the other industries in the break-down. Due to better readability, the respective figures have been placed in an annex (see annex B).

4.2 Barriers to and protection measures for sharing of data

In this section, we examine, on the one hand, barriers encountered when sharing data and, on the other hand, measures taken by respondents for protecting the shared confidential and commercially valuable data (except for trade secrets, for which we have a separate specific section (section 4.5)). We also assess possible issues of confidential and commercially valuable data sharing in the context of international/cross-border sharing.

4.2.1 Barriers for confidential and commercially valuable data sharing

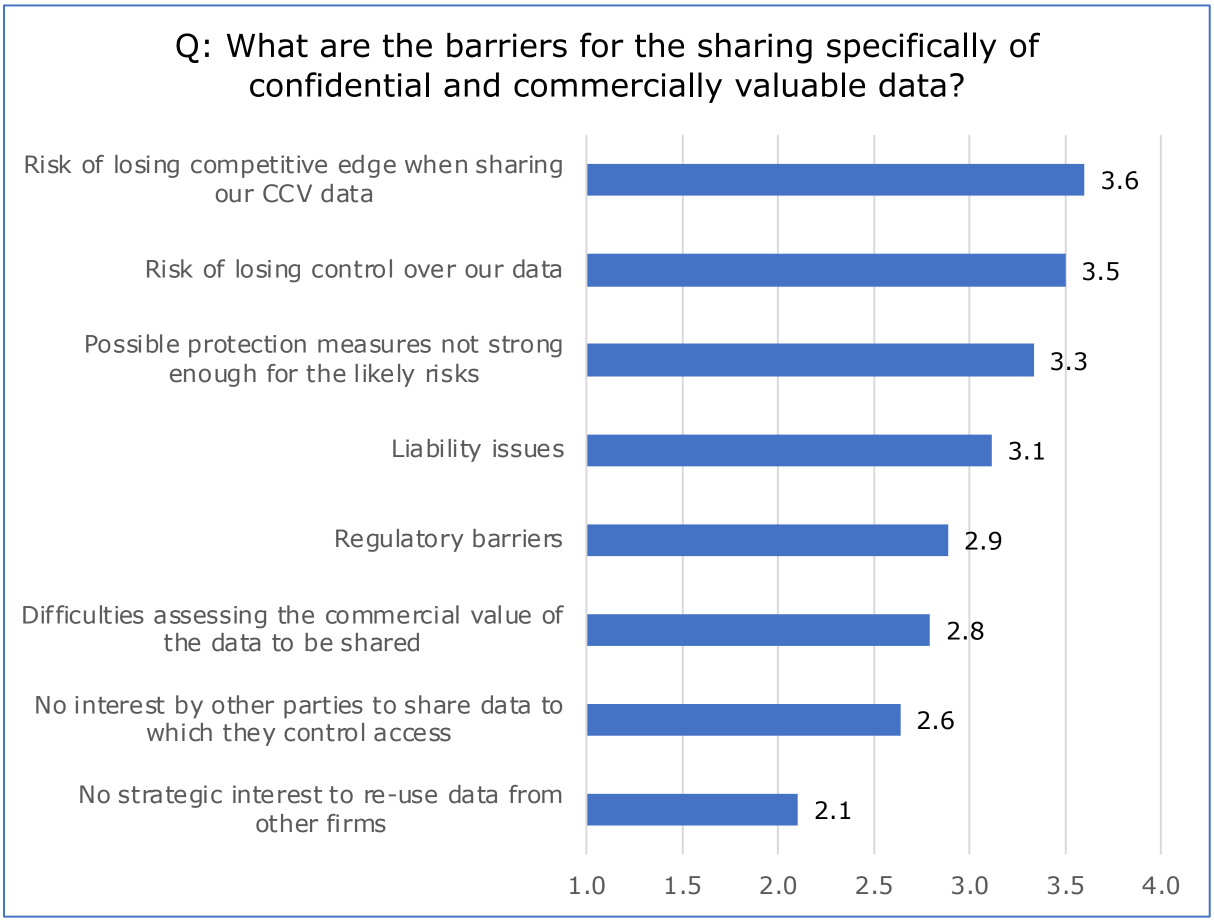
Major take-aways

- The major barrier for sharing data is risk of losing competitive edge when sharing
- "No interest" in sharing is, however, hardly a barrier

We start by looking at the barriers (see Figure 13). One can see a clear cascade of barriers sorted by relevance, the most outspoken barriers being "risk of losing competitive edge when sharing our confidential and commercially valuable data" (average rating of 3.6 on an average scale from 1=irrelevant barrier to 4=relevant barrier) and "risk of losing control over our data" (average rating: 3.5). In interviews and in the case studies, we were in this context also alerted to a conundrum whereby firms would want to share confidential and commercially valuable data, but fear that they are left out of the picture when it is about obtaining a fair share of benefits which a third obtains by using the shared data.

Ranking third on the list of barriers is that possible protection measures may not suffice in the wake of likely risks (average rating: 3.3), followed by liability issues (3.1) and regulatory barriers (2.9), hence the two latter factors being "rather relevant". Valuation issues are also only "rather relevant" (2.8), and that third parties would have no interest in data sharing were ranked as least relevant among the barriers we enquired into. Given the low number of responses in the "other types of barriers" category, we omitted this category in the chart.

Figure 13 Barriers to sharing of confidential and commercially valuable data *)



*) arithmetic means of answers on a scale from 1=irrelevant barrier, 2=rather irrelevant barrier, 3=rather relevant barrier and 4=relevant barrier
Source: Survey, n = 58-65 ("Other" category, which was omitted: n=12)

A breakdown of the barrier question by sector does not reveal highly differing response patterns.

4.2.2 Protection measures (excluding trade secrets)

Major take-aways

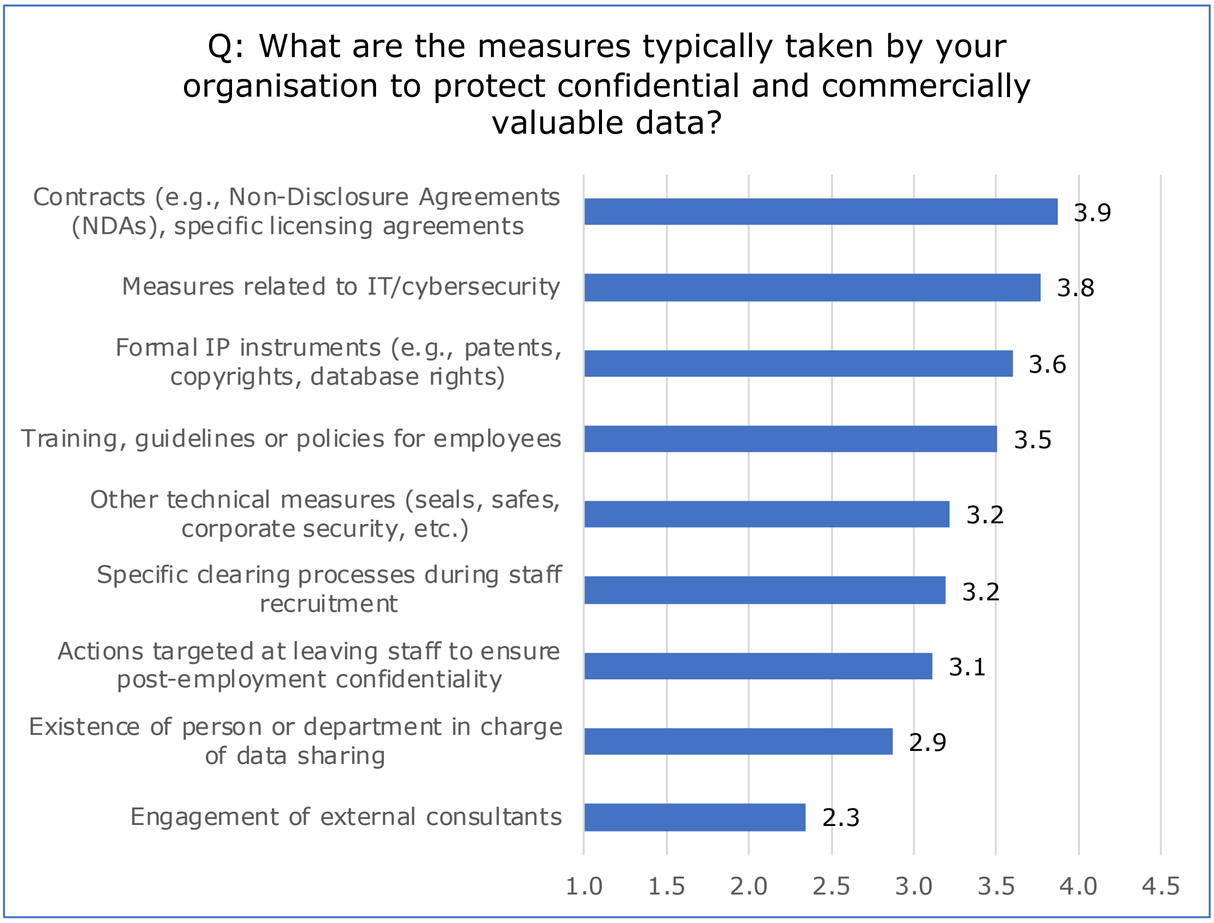
- Contracts are by far the most important means to protect shared confidential and commercially valuable data
- This is followed by IT/cybersecurity measures and formal IP protection (in cases where the data is susceptible to formal IP protection)

Figure 14 shows the assessment of different options to protect shared confidential and commercially valuable data (excluding trade secrets). A clear picture and ranking emerge:[111] Almost unanimously (average rating of 3.9 on a scale from 1=irrelevant, 2= rather irrelevant, 3=rather relevant to 4=relevant as protection measure), contracts lead the different types of measures, closely followed by IT measures. Surprisingly at first sight, formal IP, such as patents, copyrights or database rights rank third. This can be explained by the wider notion of data used for the survey (which includes also data incorporating

[111] The ranking may be even more outspoken (i.e., the distribution more skewed), because we can observe – with this question in particular – an effect by which some respondents chose to only tick the boxes for the (in their opinion) most relevant measures, and not to mark the factors they deem as (rather) irrelevant. For example, 61 answers were obtained for the measure "contracts", 55 for "clearing processes in recruiting" and only 49 for "external consultants".

know-how such as CAD files, design files and production process parameters). Factors like "training and policies for staff" (rating: 3.5), "clearing processes in recruiting" (rating: 3.2), "other technical measures" (rating: 3.2) and "actions for leaving staff" (rating: 3.1) are deemed, on average, "rather relevant". External consultants play a "rather irrelevant" role.

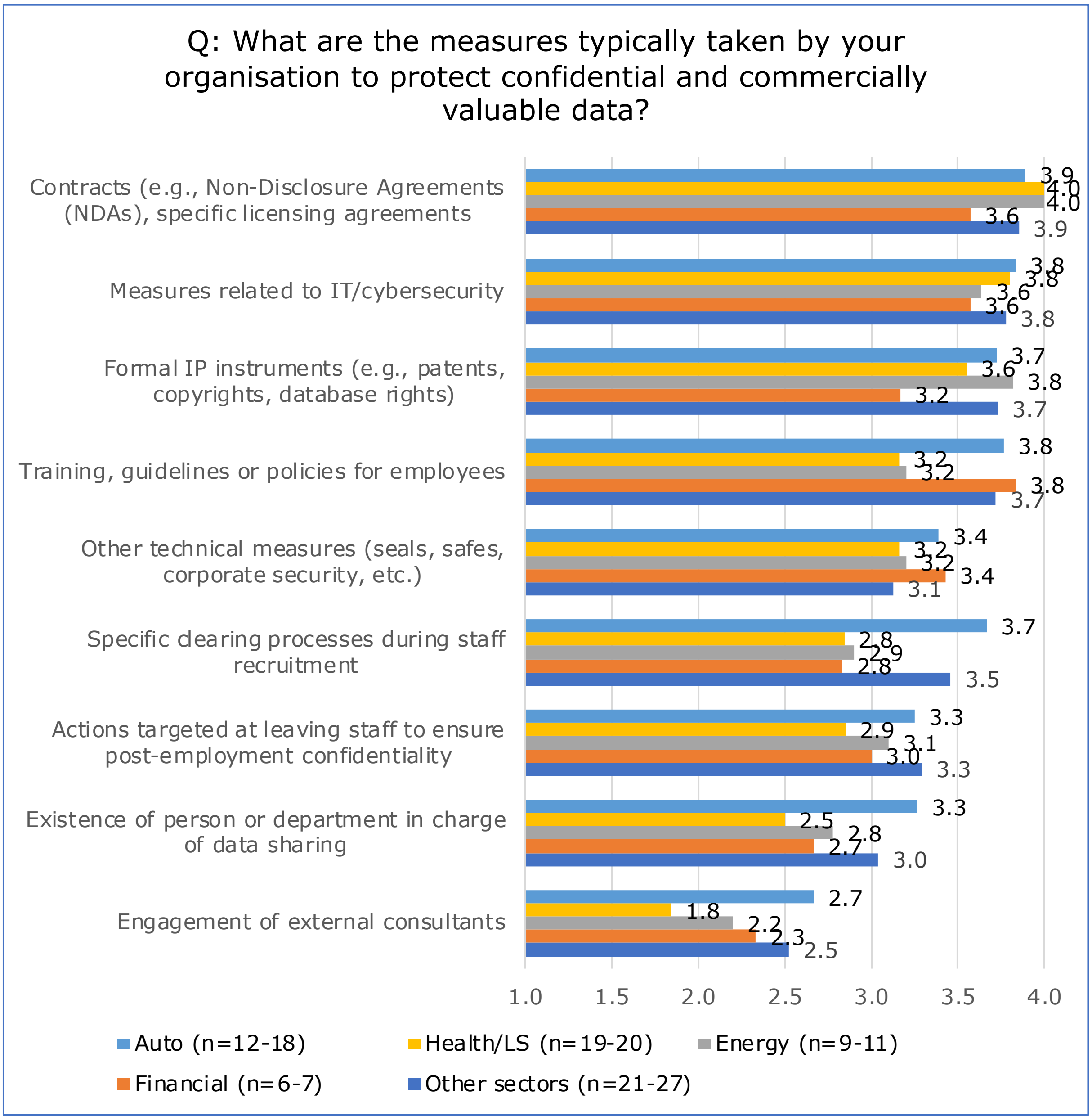
Figure 14 Relevance of different protection measures for shared confidential and commercially valuable data *)



*) arithmetic means of answers on a scale from 1=irrelevant measure, 2= rather irrelevant measure, 3=rather relevant measure and 4=relevant measure
Source: Survey, n = 55-69

A break-down of the relevance of protection measures (excluding trade secrets) by sector is provided in Figure 15. We observe only little variation in the top-ranking measures (with the exception of the financial sector, which ranks formal IP as less relevant than the other sectors, but which is not that much of a surprise, as this sector is only to a smaller extent susceptible to, for example, patent protection; the low number of responses in this sector must also be kept in mind with such interpretations). Somewhat more variation seems to be visible in the medium- and lower-ranking measures. Many of these measures are related to good practices that ensure trade secret protection. We interpret this also in the light of different experience and familiarity levels of the respondents with trade secret protection (see also section 4.3 on trade secrets usage for confidential and commercially valuable data sharing).

Figure 15 Relevance of different protection measures for shared confidential and commercially valuable data *)



*) arithmetic means of answers on a scale from 1=irrelevant measure, 2= rather irrelevant measure, 3=rather relevant measure and 4=relevant measure
Source: Survey

4.2.3 Cross-border data sharing

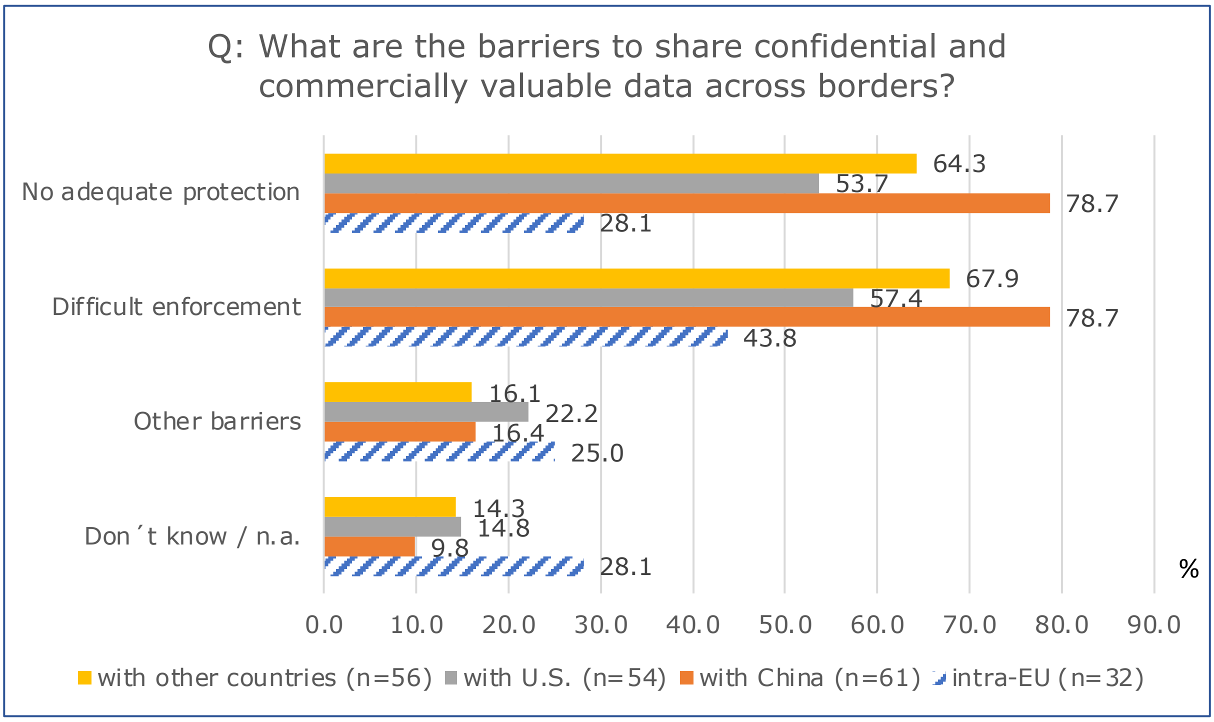
Major take-aways

- Cross-border data sharing is reportedly an issue particularly with respect to China
- However, there have been also voices that cross-border sharing with the U.S. can be challenging, too

Figure 16 shows the perceptions with regards to barriers for confidential and commercially valuable data sharing across borders. One can easily see that most problems seem to be associated with China, where 79% deem that there is no adequate protection and that enforcement is difficult, respectively. However, in the U.S., more than half of the respondents perceive that protection is not adequate and enforcement difficult, too. Countries other than China and the U.S. and outside of the EU are seen by around two thirds of the respondents as problematic.

Unsurprisingly, within the EU, the least problems are seen – the shares of 28% (no adequate protection) and 44% (difficult enforcement) do not reflect the fact that only little more than half of the respondents who answered for China and the U.S. also provided answers for the EU. It stands to reason that the shares complaining about cross-border issues in the EU are also around half of what is reported in Figure 16 (hence we used a hatched pattern in the visualization).

Figure 16 Barriers to share confidential and commercially valuable data across borders, shares of respondents *)



*) Multiple responses possible
Source: Survey

In interviews the following points also emerged:

- The hypothesis raised in the scoping interviews that national state-control and clearing procedures for "trade secrets of national interests" – e.g., in relation to China but also within Europe – would hamper cross-border sharing of trade-secret protected confidential and commercially valuable data remained a rather lone voice.
- One interview partner raised an issue in relation to taxation – it was reported that tax authorities take a close look at trade secrets as an intellectual asset of value. If they are moved, within a company group, from one country to another, proper taxation should happen. However, few companies are aware of these issues and would not have proper records and documentation of such movement of assets ready for the tax authorities.
- One interview partner stated that, in cross-border confidential and commercially valuable data sharing, it would be difficult to assess which body of law (of which country) should be used, depending on where the data is and/or should be stored (see Case Study Nr. 3).

4.3 Trade secret usage for confidential and commercially valuable data sharing

4.3.1 Use of trade secrets for protecting shared confidential and commercially valuable data

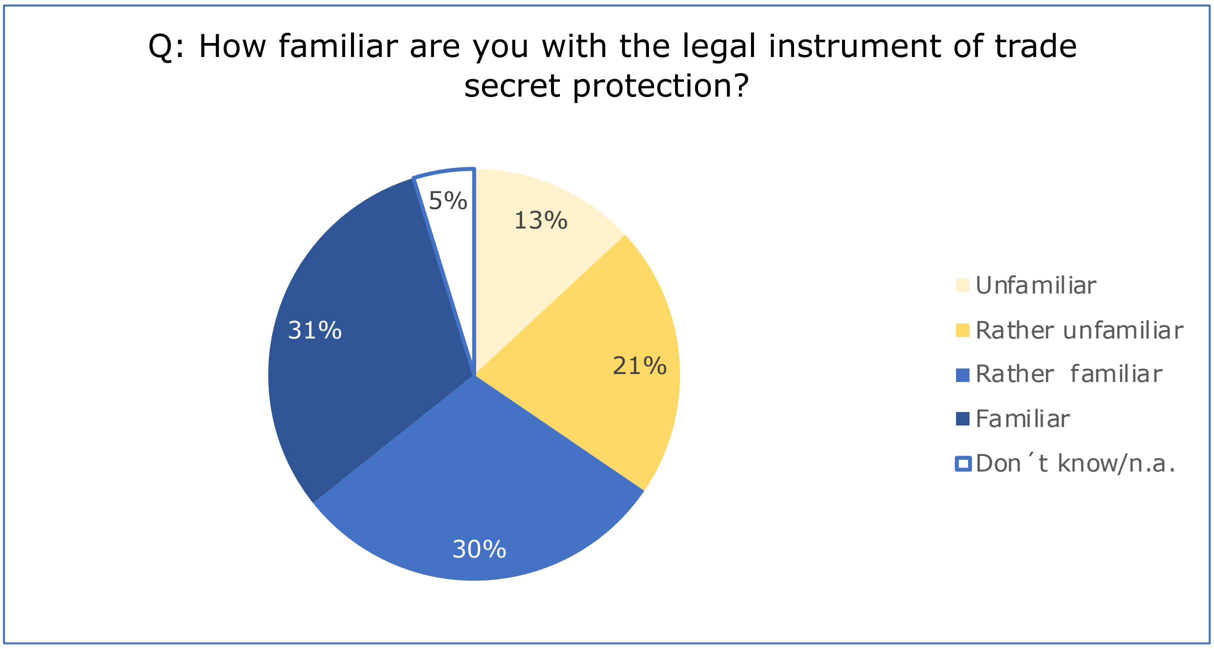
Major take-aways

- Only a rather small share of firms is well experienced in using trade secrets for protecting shared confidential and commercially valuable data
- However, 71% of firms (who are at least somewhat familiar with trade secrets) believe that trade secret protection is appropriate for protecting shared data

As a first step, we asked about the extent to which survey respondents were familiar with trade secrets as a legal tool to protect shared confidential and commercially valuable data (see Figure 17). As can be seen, 31% of the respondents declared they were "familiar" with the concept, and a further 30% stated they were "rather familiar". This means that some 39% were either "rather unfamiliar", "unfamiliar" or did not know how to answer this question.

This 39% share can be considered high, particularly given that our sampling process focused on firms and contact persons within these firms where knowledge of that concept could have been expected. However, the result resonates well with interview and case study evidence. Against this backdrop, it was frequently mentioned that *"…the topic of trade secret protection is only starting to develop"* (interview), or that departmental responsibilities for the combined topic of trade secret protection have been fragmented within the firms. Overall, we see this as one major result, explaining in large parts also the difficulties engaging firms in the survey. We will explore this phenomenon further in section 4.3.3, when we discuss barriers to trade secret usage for confidential and commercially valuable data.

Figure 17 Familiarity with trade secret protection for confidential and commercially valuable data, firms in %



Source: Survey, n = 84

A sectorial breakdown of the question on familiarity with trade secret protection for confidential and commercially valuable data is provided (see Figure 18). Among the four specific sectors we enquired into, it is the health and life sciences where familiarity seems the most to be most prevalent. The energy sector seems considerably less familiar with trade secret protection, despite data sharing being a (developing) topic there. The charts for the financial sector (and also energy) allow no solid conclusions from the survey, given the low number of responding firms. In both sectors, familiarity can be on average considered low. An example of a firm heavily involved in data sharing in financial services but not considering trade secret protection is provided below.

Case Study Nr. 5 – Insurance company – heavy in data sharing, light with IP and trade secrets

Sector:	Financial services
Type of organisation:	Large firm
Type of data shared:	Various
Data shared with:	e.g., health care organisations
Use of trade secrets:	No (of minor importance)

Insurance companies are generally data-driven companies. The entire industry thrives on knowing the risks of policyholders better than the policyholders know them themselves and using this expertise for product design. Policyholder data (personal data about the policyholder and the customer's previous activities or product use) and external data are essential for the calculation of the products and are incorporated into the product design and the business model.

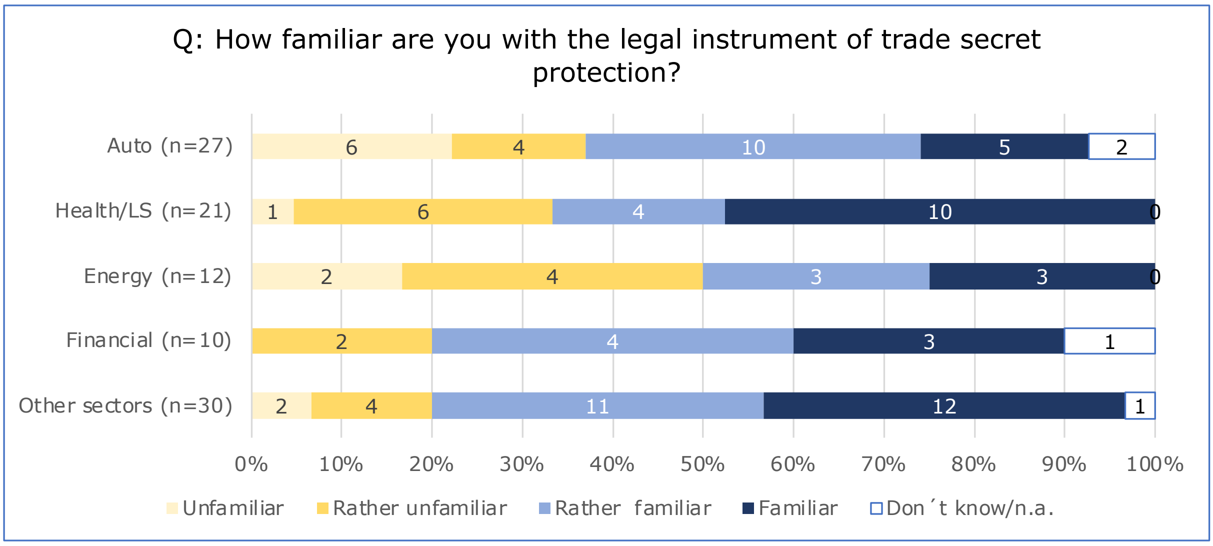
Data is often shared with third parties. These are, for example, intermediaries, brokers but also other insurance companies and regulatory authorities. However, data is also shared with hospitals in the case of health insurance and in the fight against fraud, shared databases with the insurance association play a major role.

When dealing with confidential and commercially valuable data, it is important to divide the data into categories. For example, a distinction is made between general data, confidential data and strictly confidential data. Specific confidentiality levels are set for each of these forms, and technical safeguards and contractual elements are defined accordingly. There is no standardised process for identifying confidential and commercially valuable data.

When confidential and commercially valuable data is exchanged across borders, the legal requirements in the recipient country must be met. When data is exchanged, the categories of data (categories of data processed, categories of recipients, categories of data subjects) must be identified to ensure unambiguous classification. For example, when describing the categories of recipients, care must be taken to ensure that verification of lawfulness is possible. This is very complex due to the different legal bases and very costly for insurance companies. In principle, a very restrictive approach is taken when sharing confidential and commercially valuable data, and only absolutely necessary data is exchanged with business partners, but also with regulatory authorities. Finally, patents, copyright, database rights and trade secrets for the protection of confidential and commercially valuable data are of minor importance to insurance companies or are not seen as relevant for this insurance company.

By contrast, in the "other sectors" category, we observe some 77% (23 out of 30 respondents) to be "rather familiar" or "familiar" with the topic. Our interpretation – as said, also considering qualitative evidence – is that there are sectorial differences, but above all and across all industries, there is a smaller group of firms who have already more extensive experience with the topic, while the remainder are either catching up or the topic is not (yet?) relevant for them.

Figure 18 Familiarity with trade secret protection for confidential and commercially valuable data, firms in absolute numbers, by sector

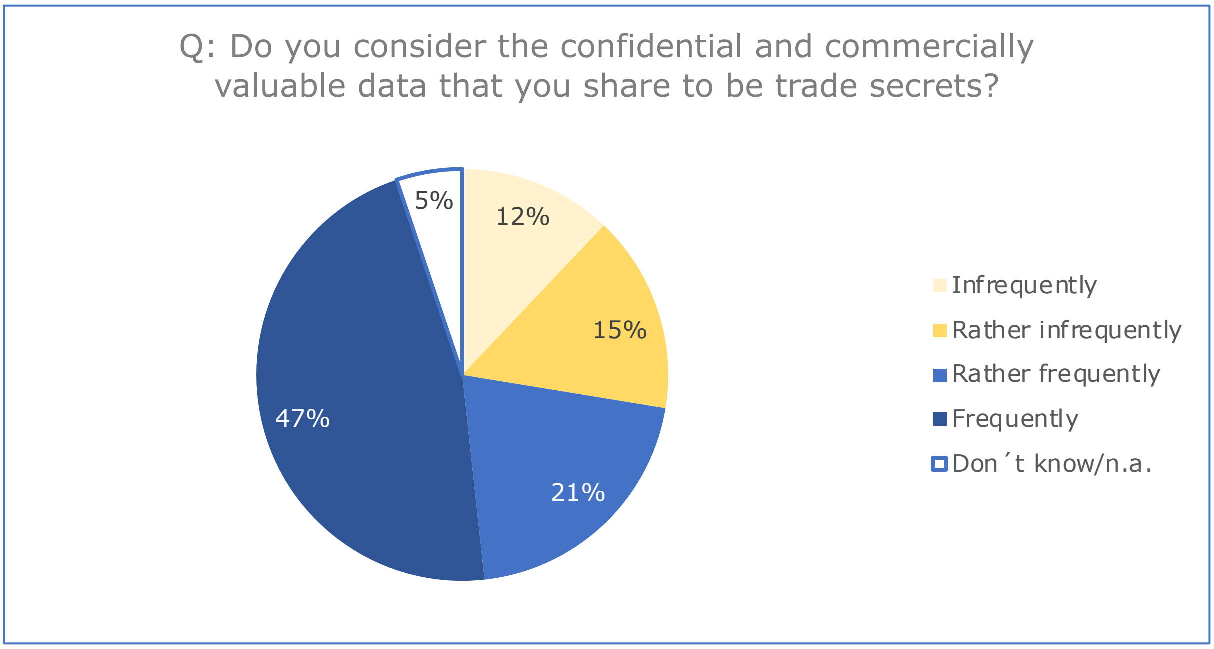


Source: Survey

In a next question, we asked in the survey whether the confidential and commercially valuable data that has been shared qualifies for trade secret protection (see Figure 19). Note that this question (and all ensuing questions in this section which pertain directly to trade secrets) was not posed to firms who declared that they were not familiar with trade secrets or answered the familiarity question with *"don´t know/n.a."*. This is because the respective respondents would not have been able to answer the follow-up specific questions on trade secrets.

As can be seen, some 47% said that the shared confidential and commercially valuable data would qualify "frequently", and for another 21% *"rather frequently",* for trade secret protection. Only some 12% stated this to be *"infrequently"* the case. We interpret this result in a rather straightforward way, namely that, for those who have at least some level of knowledge/familiarity with trade secrets and confidential and commercially valuable data sharing, in a large number of cases, trade secret protection is or could be used to protect shared data.

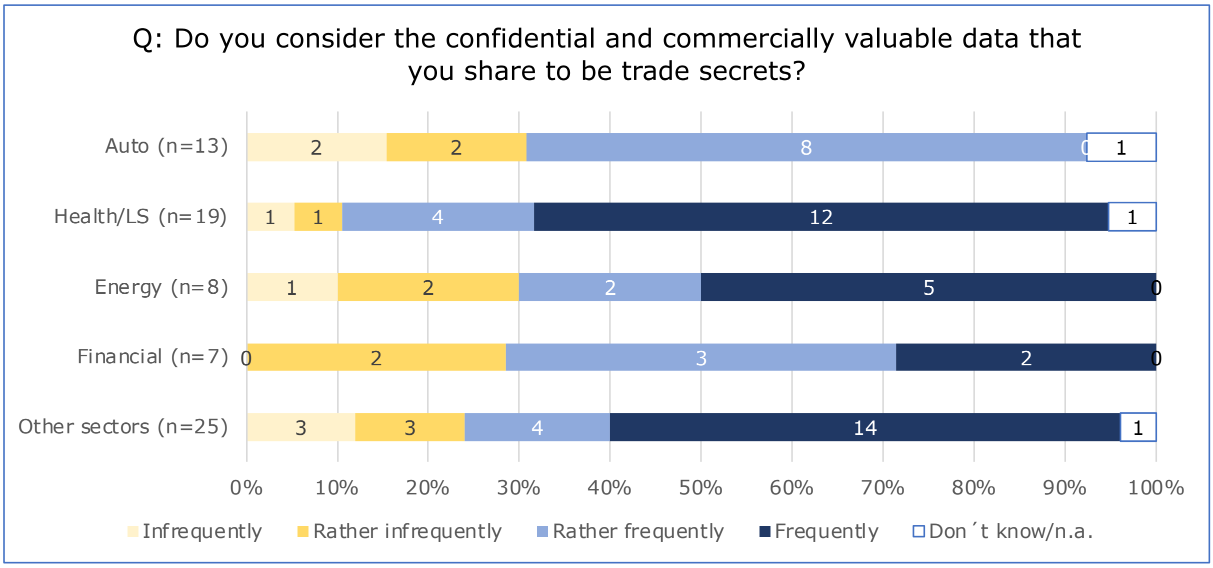
Figure 19 Extent to which shared confidential and commercially valuable data qualifies for trade secret protection, firms in %



Source: Survey, n = 58

Figure 20 reveals differences by sector. Health and life sciences stand out again as the sector where the shared confidential and commercially valuable data most likely qualifies for trade secret protection. In the other three explicitly scrutinised sectors, we not only observe lower frequencies of firms where data qualifies "rather frequently" or "frequently" for trade secret protection, but also a lower number of respondents – for us, again proof that the topic is mostly starting to develop and relatively few firms can reliably answer the question. The "Other sectors" sector – comprising firms from a variety of sectors, who seem to share a particular interest in trade secret protection for shared confidential and commercially valuable data – has by contrast a relatively large share (around 72%) who stated that trade secrets would qualify for their shared confidential and commercially valuable data.

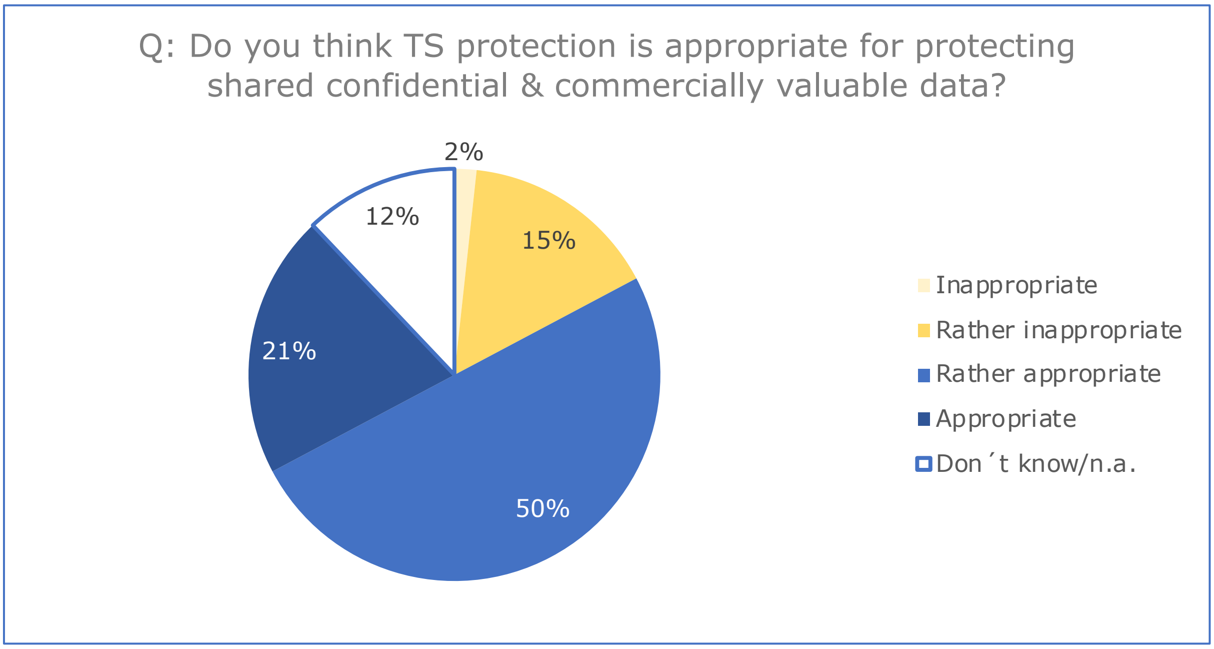
Figure 20 Extent to which shared confidential and commercially valuable data qualifies for trade secret protection, firms in absolute numbers, by sector



Source: Survey

In a third step, we looked at whether respondents deemed trade secret protection as appropriate for the protection of shared confidential and commercially valuable data (see Figure 21). 50% answered this question as "rather appropriate", and (only) 21% reported trade secrets to be "appropriate". 15% answered with "rather inappropriate" and only 2% as "inappropriate". A rather large share could not answer this question (12% answered "don´t know/n.a.").

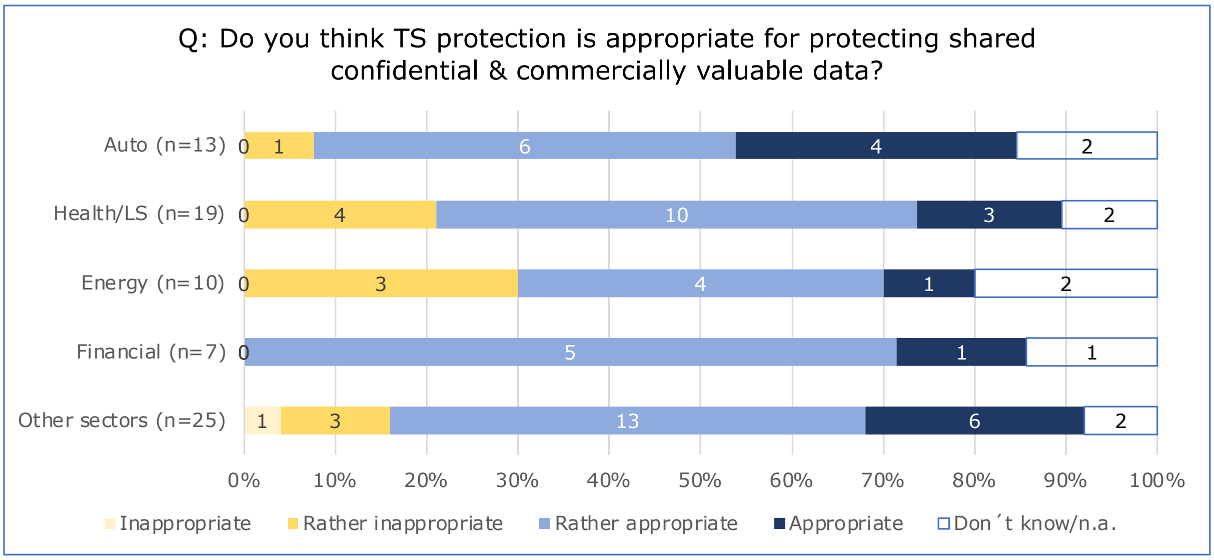
Figure 21 Appropriateness of trade secrets to protect shared confidential and commercially valuable data, firms in %



Source: Survey, n = 58

The sectorial breakdown for the question on appropriateness of trade secret protection is provided in Figure 22. Across all sectors only a minority of firms find trade secret protection to be fully appropriate, with respondents opting mostly for the "rather appropriate" category. We will discuss possible reasons for this behaviour when we discuss the motives and barriers to use trade secret protection for shared confidential and commercially valuable data in sections 4.3.2 and 4.3.3.

Figure 22 Appropriateness of trade secrets to protect shared confidential and commercially valuable data, firms in absolute numbers, by sectors



Source: Survey

4.3.2 Motives to use trade secrets for shared confidential and commercially valuable data

Major take-aways

- The most important motive to use trade secrets for shared confidential and commercially valuable data is to prevent misappropriation by third parties
- This followed closely by the motive to have an additional safety net, should protection with contracts fail

Eventually, we asked survey respondents about their motives to use trade secrets for shared confidential and commercially valuable data (see Figure 23). For easier interpretation, we computed arithmetic means of answers obtained on a 4-tier scale from 1=irrelevant as motive, 2=rather irrelevant as motive, 3=rather relevant as motive to 4=relevant as motive.

In the lead is the motive to prevent misappropriation of trade secrets by third parties (average rating: 3.5), almost on a par with the motive of an "additional layer of protection" on top of contracts (average rating: 3.4). Trailing behind only slightly are the factors "to increase control over the shared confidential and commercially valuable data" and "to enable joint R&D and innovation-seeking collaborations in full trust" (both 3.3, respectively), which is followed by "to improve the wording/drafting of contracts" (average rating: 3.0). All these factors received an average rating of 3.0 or above, which means that they are seen as "rather relevant" to "relevant motives". The factor of ensuring prolonged protection beyond, for example, the 20-year time limit of patent protection, had an average score of 2.8, but could therefore still be seen as a "rather relevant" factor for many firms. Using trade secrets for finance and fund-raising purposes[112] fared, on average, as only a "rather irrelevant" motive.

We omitted the category of "other motives" because there were only very few responses in this category, although the few responses provided some interesting thoughts.[113]

In interviews, we were also alerted to new drivers for trade secret protection:

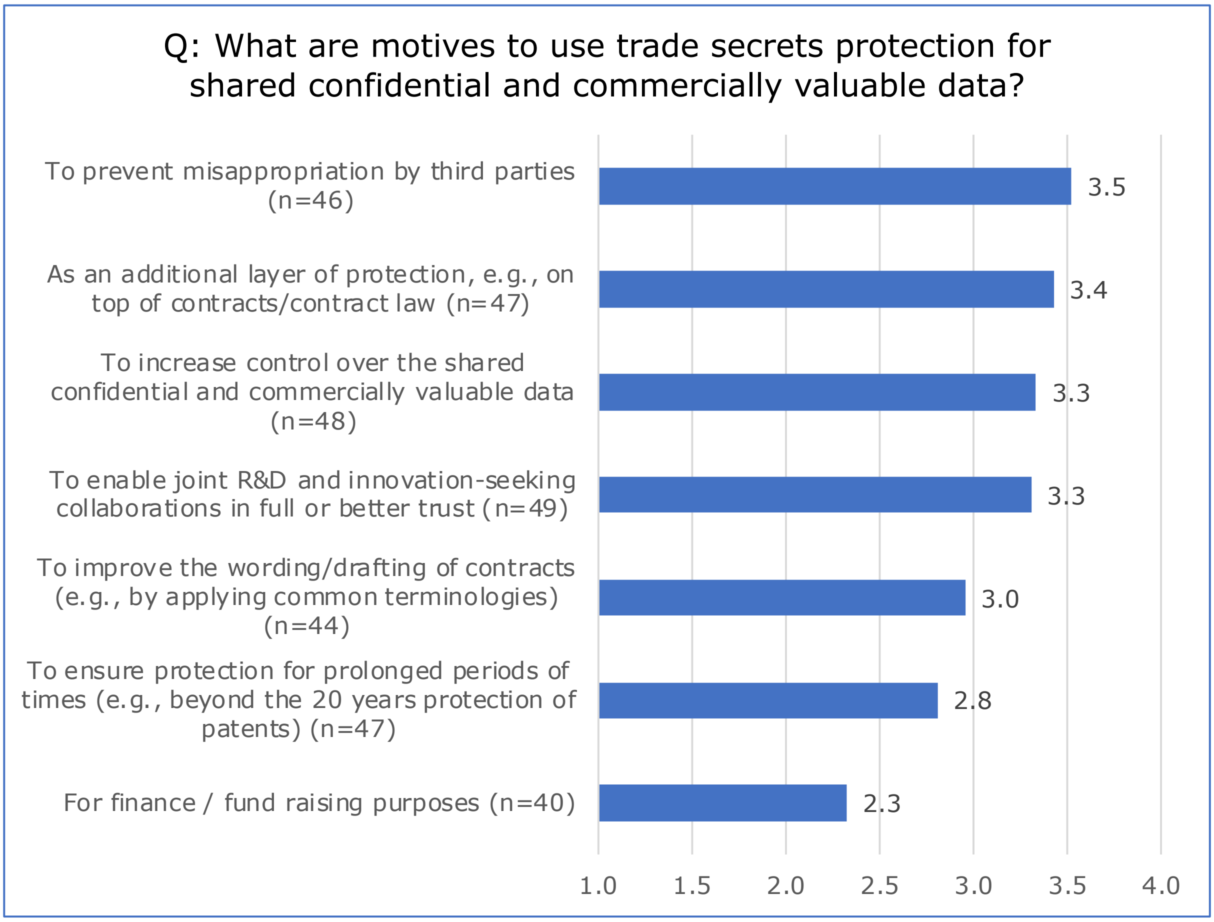
- *"Going beyond NDAs"* (interview), in this context, is understood as a trend where companies need to demonstrate, beyond the mere signing of a contract and/or NDA, that they can manage trade secrets. Hence, this trend corresponds to an audit or certification process of the respective firm´s capability to handle trade secrets and hereby indirectly also drives trade secret usage.
- Trade secrets were also said to be useful tools for protecting fundamental rights (see Case Study Nr. 6 below) and for the protection of dynamic data.

As a bottom line, we can observe that there is breadth of common motives to use trade secrets, which are in line with results from interviews. These identified the second layer of protection after contracts (interview), the improvement of the wording/drafting of contracts, as well as the prevention of misappropriation by third parties as major factors speaking for trade secrets.

[112] One interview partner noted specifically that trade secrets make up part of the value of a company and provide some *"guarantee"* that *"…money invested is somehow protected / guaranteed"*. (interview). However, in this context, there are valuation issues to be considered.

[113] For example, a mobility service provider using cars stated that trade secrets are a good means to protect fundamental rights (in cases where GDPR protection would not be any more applicable) as well as specific forms of dynamic data absent software patent protection.

Figure 23 Motives to use trade secret protection for shared confidential and commercially valuable data *)



*) arithmetic means of answers on a scale from 1=irrelevant as motive, 2=rather irrelevant as motive, 3=rather relevant as motive and 4=relevant as motive
Source: Survey

Case Study Nr. 6 – Mobility service provider in the automotive sector and its use of trade secrets for protecting dynamic data and fundamental rights

Sector:	Automotive (mobility services)
Type of organisation:	Large firm
Type of data shared:	Location data
Data shared with:	Maps data suppliers
Use of trade secrets:	Yes

The case study at hand is about a firm offering mobility as a service (ride-hailing, food, delivery, package delivery, couriers, etc.).

The major type of data for which sharing is of interest is location data. Such data is acquired from smart phones (i.e., mostly machine-generated). The data could support, for example, city planning, by helping to understand the behaviour of riders when they move around. The location data on movements resulting from one individual trip may not be hereby of so much interest but aggregating the data and observing it over time will reveal interesting patterns. By its nature, such location data is personal data which, however, can be in principle transformed into non-personal data through abstracting – for example, by leaving out the start and end points of a trip. This procedure to obtain derived data is not perfect though. A case in point is less densely populated areas. Leaving out start and end points could eventually still lead to the identification of movement patterns of individuals identifiable by name through contextual analysis.

Given the potential for exploitation of the location data, there is demand (e.g., from city planners) for the company to share the data. These demands could be technically met by a variety of channels, including FRAND licensing arrangements; through a marketplace; and/or through (forced) regulation.

Location data is therefore of principle economic value, it is secret and protective measures are taken by the firm to keep the data secret.

Following this, such data is trade-secret protected, particularly if it refers to the derived/abstracted data where GDPR does not apply anymore. In this context, one principal argument of the company regarding the utility of trade secret protection is that trade secrets then help secure human rights for both riders and drivers using the firm offerings – if data sharing is not well governed, there is the risk that personal data is revealed (re-engineered through said contextual analysis) and potentially abused by a third party. Regulating access through trade secrets may, therefore, provide a shield for human/fundamental rights of individuals and/or groups of individuals.[114] Against this backdrop, the company states "*…that for any mandatory regulations legislators should take a very careful approach catering for the contextual factors, which is very difficult"* (interview), so the company clearly favours voluntary data sharing governed by contracts.

Third party IP rights – and here again trade secrets, but also database rights – are implicated in this case, mainly those of map makers. Their know-how (and IP) is needed to turn GPS coordinates into actual addresses. A major part of the value offering of map makers is that they keep the maps constantly up to date, i.e., as high-quality dynamic data. This requires constant investments. The company sees this aspect also as the prime reason why free/open map data (even if created and offered by government) can never reach the quality of the data and offerings of private map providers.

Against this backdrop, trade secrets also help shield and monetise investments of map makers in the interest of the mobility service company as a client. Consequently, in the context of such dynamic data, trade secrets are a facilitator, even enabler, of data sharing between firms, "*…enabling others to build offerings on the shared data"* (interview). The company therefore opines that future legislation dealing with data sharing should follow the model of the GDPR which sets out limits should the GDPR infringe on the (IP) rights of others. Equivalent clauses should be copied also into other pieces of legislation, and it would be beneficial, if it is explicitly spelled out that trade secrets are an example of such (IP) rights of others.

4.3.3 Barriers to use of trade secret protection for shared confidential and commercially valuable data

Major take-aways

- The major barriers speaking against trade secrets are reported to be enforcement related: difficulty to track or control the use of the shared confidential and commercially valuable data; difficulty assessing whether a trade secret has been misappropriated; unclearness whether enforcement of trade secrets is legally efficiently and effectively possible
- There is some insecurity with firms stemming from lack of developed jurisprudence and/or from perceived ambiguity in the wording of the TSD[115]
- However, given the fact that many firms have only started to build up experience in the field (and could answer this question), lack of awareness and know-how is likely to be also a significant barrier

While the preceding section looked at motives to use trade secrets for shared confidential and commercially valuable data, this section looks at the respective barriers. Survey answers lead to the picture displayed in Figure 24. In contrast to the motives, we can observe a clear ranking of barriers. Rated as the most pronounced barriers, we see the leading factor as "difficulty to track or control the use of confidential and commercially valuable data" (average rating: 3.5), which is followed by "difficulty assessing whether a trade secret has been misappropriated" (3.3) and "unclear whether legal enforcement of trade secrets is effectively and efficiently possible" (3.2).

[114] However, it should be noted that this stance has been also met with scepticism. The main argument is that either the GDPR (or other data protection/ privacy rules) apply and data protection/privacy is secured, or it does not apply because there is no personal data (and in that case there is no problem).

[115] These perceptions are specifically reflected upon in the legal analysis in chapter 5.

All three are therefore, at least to different extents, enforcement related. This resonates well with answers from interviews, where a larger number of interview partners were unsure about enforceability, due to, for example, lack of ECJ decisions in dedicated trade secret cases. Specific reference was made in the interviews in relation to the actual defining criteria of trade secrets:

- In relation to the criterion of having adequate protection measures, it is unclear how "reasonable steps" for maintaining secrecy will be assessed in practice. One issue that we could see lingering in this context is that the definition of trade secret protection measures in trade secret law is binary (either protection measures are "reasonable" or "adequate" or not), while in practice most firms we interviewed differentiated between different levels of confidentiality depending on the value of the to-be-shared confidential and commercially valuable data protected – hence, some firms would opt for very strict protection measures for "very valuable" data, while security measures would be less stringent in other cases.
- In relation to the criterion of "commercially valuable", one issue seems to arise from a situation whereby data – which has initially no value – is shared, and later, a third party uses this data with a break-through innovation to create revenue, turning the initial data valuable. Would this shared original confidential and commercially valuable data, due to the potential value it could have, still fulfil the criterion of "commercially valuable information" and be protected by trade secrets? Many firms believe such "original" data to be of no or little value, and – apart from the processing step, which often relates to a piece of software, in advanced cases to ML/AI algorithms – assess that this kind of data is treated differently by trade secret law, i.e., though confidential, it does not constitute a trade secret (while *"…in practice the firm should treat trade-secret protected data and confidential non-trade-secret protected data equally"* (interview)). The difference between trade secret protected shared data and "just" confidentially shared data is also discussed in the following Case Study Nr. 7.
- The preceding bullet points lead also to the question of how a company can ensure control over the shared (and trade-secret protected or only confidential) data, particularly in terms of when value is created – how can a firm ensure that it obtains a fair share of the benefits created with the data that it provided?

Case Study Nr. 7 – Machinery firm in the automotive sector using trade secrets as default protection measure and highlighting the subtle differences between shared confidential data that is trade secret protected and shared confidential and commercially valuable data that is not trade secret protected

Sector:	Automotive sector (supplier)
Type of organisation:	Large firm
Type of data shared:	Production process data / machine-generated
Data shared with:	Clients, research partners
Use of trade secrets:	Yes

The company in this case study is a manufacturer of machines with which high-tech components for use (also) in cars are created. These machines produce large amount of data (also including image data from cameras) which is needed to control the machines and to optimise production processes in client factories. Even small improvements here can translate into considerable commercial gains, e.g., in terms of cost advantages by managing wear and use of the machines and ensuring quality output. The data under consideration is hence mostly sensor-generated data with no nexus to personal data.

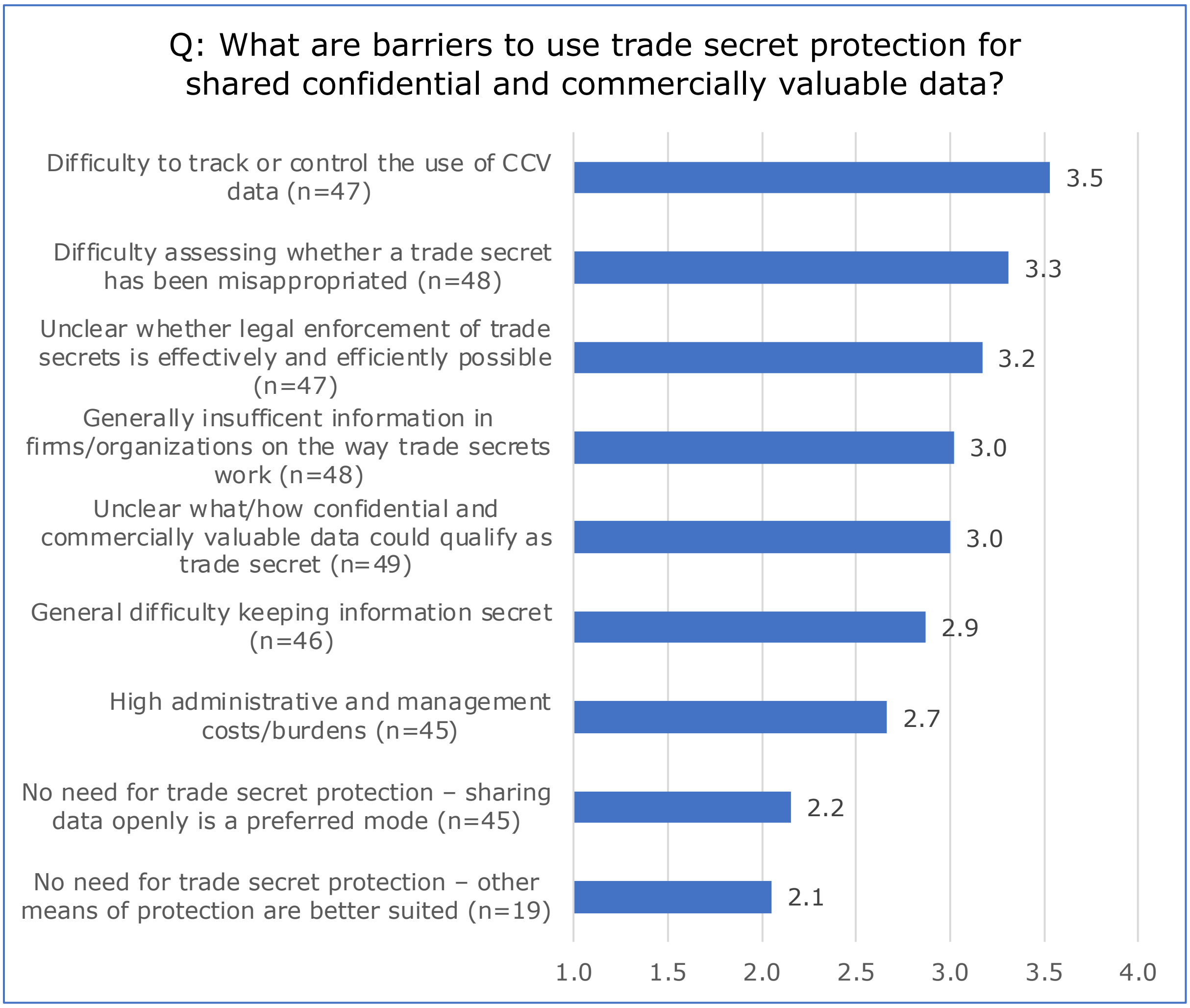
While there is therefore a clear motive to share data between firms, data sharing has so far remained a rather difficult task. Client firms fear for their own trade secrets and confidential data, and while they are interested in improving their production processes, they often do not reveal important data (e.g., in relation to quality control) which could lead to respective improvements. Clients also demand full access to all data of the machines, which is conversely also provided only partially by our case study company. Hence, there are typically tedious negotiation process in place to regulate data access rights and the modes of data sharing (such as certain data being shared only offline) with contracts. The fact that the customers are (large) firms and not consumers, however, *"…is at least* *somewhat simplifying things"* (interview). Nonetheless, the topic of IP and data sharing is *"…a hot topic which is currently developing in our industry."* (interview).

There are organisational and managerial ramifications of the confidentiality obligations arising from the said negotiations as *"…each piece of information given to us by our clients cannot be passed on."* (interview). This also applies to information flows within the firm – there are separate accounts for each client, their contact persons and liaisons must be different and business operation/contacts are also kept organisationally separate. As the R&D department operates as a central unit, information from different customers eventually makes its way to overall improvements of the machines which benefit the whole client base. The increasing need for data sharing has also rather recently led to the IP department becoming also responsible for data (sharing) from a legal point of view, with an ensuing work division that the IP department, in an iterative process, defines company-internal processes and the IT-department is tasked with implementation (e.g., through software, cryptography).

The company explains its protection strategy for shared data by explaining that the default mode are trade secrets: *"Everyone owns its data, protected through trade secrets, and data is prima facie not to be shared. Contracts hereafter soften this situation and create the exceptions and conditions by which specific kinds of data are then shared and exploited – a situation like deer hunting, where the deer can only be hunted in one´s own woods, even if the deer moves freely between different woods."* (interview). This means that trade secret protection and access to them is applied through contracts. In addition to trade secrets, the firm makes heavy use of TPMs of all kinds. Apart from data being subjected to trade secret protection, trade secrets are also an important means to protect the Machine Learning algorithms used to create derived/processed data.

Interestingly, the company reports that the industry often does not differentiate well between trade secrets and confidential information. Single data is not commercially valuable (hence not trade-secret protected), but the complete data, the "whole picture", is of value. Similarly, original data is not (that) valuable, while data derived/processed from the single data has significant value. The distinction between confidential information and trade-secret protected data is, for the firm, however subtle and critical at the same time. The major point is that both types of data/information are and should be protected, but only one of them enjoys the additional trade secret protection. Great care must be taken to also protect the original (confidential) data: *"Trade secrets and confidential data are theoretically something different, but in practice both should be managed the same way."* (interview).

Figure 24 Barriers for using trade secrets to protect shared confidential and commercially valuable data *)

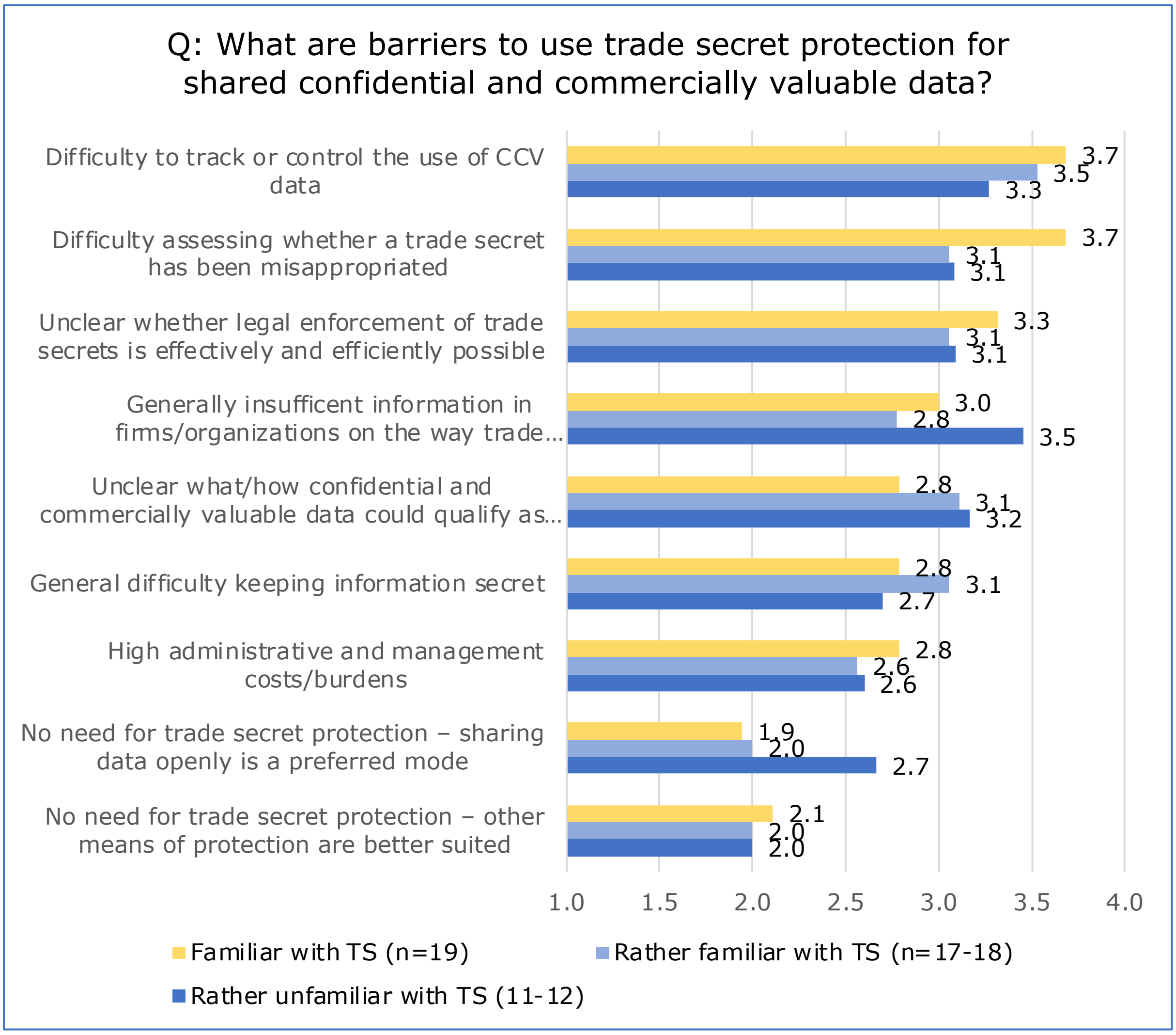


*) arithmetic means of answers on a scale from 1=irrelevant as motive, 2= rather irrelevant as motive, 3=rather relevant as motive and 4=relevant as motive
Source: Survey

Following the "enforcement-related cluster" barriers, we find two factors that were rated as "rather relevant" (with an average rating of 3.0, respectively): *"generally insufficient information in firms/organisations on the way trade secrets work"* and *"unclear what/how confidential and commercially valuable data could qualify as trade secret"*, which was followed by *"general difficulty keeping information secret"* (rating: 2.9).

We believe especially the first two factors (the ones rated each 3.0) to be underestimated as barriers, in light also of interview evidence, as we see here a selection bias towards the more experienced trade secrets users in our sample. In this context, it stands to reason that the two factors would have been rated far higher in a more general population, e.g., had this question also been posed to those respondents who declared they were "unfamiliar" with trade secrets. We find an indication to that end when limiting our answers only to those respondents who said they were "rather unfamiliar" with trade secrets. In this group, we find one of the most outstanding barriers for trade secrets use to be exactly the factor *"generally insufficient information in firms/organisations on the way trade secrets work"*, with an average rating of 3.5 on our 4-tier scale (see Figure 25).

Figure 25 Barriers for using trade secrets to protect shared confidential and commercially valuable data, by level of familiarity with TS protection *)



*) arithmetic means of answers on a scale from 1=irrelevant as motive, 2=rather irrelevant as motive, 3=rather relevant as motive and 4=relevant as motive
Source: Survey

We observe that the response patterns to this question are very similar across the sectors – one tendency to notice is that the health and life sciences sector seems a bit less concerned about the "know-how"-related barriers, indicating perhaps that this sector, at least in our sample, is more professionalised in this topic.

Interviews also provided other interesting barriers to share confidential and commercially valuable data and protect these through case studies. One aspect were antitrust regulations: There is apparently an issue when the exchange of data which is confidential and commercially valuable (confidential and commercially valuable) is fostered in the EU, while at the same time such sharing could result in an antitrust case (see also Case Study Nr. 8 – however, it seems that this fear is more of theoretical nature and not reflected in an actual antitrust case).

Case Study Nr. 8 – OEM firm in the automotive sector stating that data sharing follows investment principle and is not available for sharing "as such", while also raising antitrust issue as a barrier to confidential and commercially valuable data sharing and trade secret usage

Sector:	Automotive sector (OEM)
Type of organisation:	Large firm
Type of data shared:	Various
Data shared with:	Suppliers, partners from other industries (insurance companies)
Use of trade secrets:	Yes

The firm in this case study is an EU-based automotive OEM. Currently, confidential, and commercially valuable data is shared based on stand-alone license agreements and as an integral part of broader agreements. Currently, NO data is generated and processed without purpose, since the generation and processing of confidential and commercially valuable data requires significant investment. Therefore, the efforts necessary to generate and process data that is then "ready to share", must be evaluated from a business perspective, in particular, a return-on-investment perspective. Currently, NO data is "just available" without any prior investment.

Typical motives to share confidential and commercially valuable data are to establish a common basis for partners to create better innovations. Sharing of data on a bilateral level generally happens to create value on both sides, i.e., there is no selling of data as such (at least not yet as there are no markets). There is always own business purpose (but only if it is legally permitted to share, e.g., due to antitrust laws). There are also typical reasons (barriers) not to share confidential and commercially valuable data: confidential and commercially valuable data is considered trade secrets and confidential know-how, which is of strategic relevance and can, therefore, not be shared from a business perspective and/or an antitrust perspective.

Besides the sui generis protection of databases, trade secret protection (under the EU TS Directive) is the second statutory pillar for protection of confidential and commercially valuable data for innovative companies. These two legal means are, next to the contractual means, most relevant for handling the sharing of confidential and commercially valuable data; trade secrets and database protection are the legal basis for justification of certain data licensing agreements, in particular, justification of, for example, "field-of-use" restrictions, that in consequence foster data sharing; trade secrets are, therefore, a very relevant instrument for secrecy and know-how protection.

Typically, contractual, and legal measures are undertaken to protect confidential and commercially valuable data. However, these measures are not considered to be adequate in the face of the risks associated with the loss of secrecy: Trade secret protection does not allow for open-data-initiatives, since "open" data sharing will automatically end trade secret protection. Unlike open-source-initiatives, where software copyrights provide a clear IP framework, IP protection (sui generis right for database protection) for data is relatively limited, and its scope of protection is not entirely clear. The firm states that adequate protection of investments is key for innovative businesses. The willingness to share confidential and commercially valuable data is directly related to the level of protection for confidential and commercially valuable data holders and a clear legal framework. Only if the current level of protection for confidential and commercially valuable data under the database directive and the TSD will be maintained and further developed to adequately protect the investments associated with the generation and processing of data, innovative businesses will become more open to share confidential and commercially valuable data. Without sufficient IP and know-how protection, most businesses will simply rely on and maintain the secrecy of their confidential and commercially valuable data.

The firm noted, eventually, that several EU initiatives try to encourage businesses to share confidential and commercially valuable data which obviously consist of confidential and commercially relevant information. At the same time, though, the exchange of such information between certain businesses is a major antitrust issue (see horizontal guidelines). The question therefore remains for the firm of where the EU wants to draw the line.

5 The empirics revisited – a legal assessment and prospective issues

5.1 Overview

In this section, we revisit the results of the preceding chapters – particularly the empirical results of section 4 – and analyse these through a legal lens. We address the definition of trade secret and its application in the data economy; we note the absence of harmonisation when it comes to confidentiality and non-compete obligations on employees and ex-employees and explore the relationship of contract and trade secrets law. In addition, we contrast the situation in the EU with that in Japan and in the U.S. and look ahead to the proposed EU Data Act. The legal analysis hereby draws on desk research, the analysis of legislation, case law and secondary literature, as well as, for the assessment of the situation in Japan and the U.S., interviews with experts on Japanese trade secret and competition law (three interviews) and U.S. experts (one interview).

5.2 The definition of 'trade secret'

An overwhelming trend revealed by the empirical data is that, despite the introduction of a homogenous legal definition of "trade secret" by Article 2(1) TSD to address the perceived heterogeneity of trade secrets definitions in EU Member States,[116] there is still considerable uncertainty in industry about what may constitute a "trade secret". Of particular concern was the meaning of *potential* commercial value and *reasonable steps* to keep the information secret.

One may speculate about why there is uncertainty regarding the meaning of "trade secret", especially in the context of the modern data economy. The first is that, while Article 2(1) TSD is not a new definition, because it is comparable to Article 39 TRIPS and broadly reflects a "recurrence of certain common requirements" that existed in Member States laws prior to harmonisation,[117] it is a new EU obligation that has not yet been interpreted by the CJEU. While there is a developed comparative jurisprudence of "trade secret" in the United States[118] and, to a lesser extent, in Japan (see section 5.6 below), EU industry participants may not feel confident in assuming that the CJEU or national courts in Member States will take a similar approach. Second, comparative jurisprudence tends to focus on know-how and information generally and has not yet grappled with the complexities of the data economy. Therefore, the applicability of trade secrets to the data economy is still relatively untested and unexplored in litigation. Legal scholars have begun to consider the role of trade secrets protection in relation to machine data and AI, but this remains an emerging area of scholarship[119] and without any judicial clarification in the EU.

[116] See EUIPO, *The Baseline of Trade Secrets Litigations in the EU Member States* (2018), pp. 5-6 and remainder of the report. See also Martinis, et al, 2013, pp. 4-5 and 24-26.

[117] Martinis, et al, 2013, p. 5.

[118] Analysing the lessons from U.S. trade secret law for the 'reasonable steps' requirement of 'trade secret' see Beale, A. & Foulser McFarlane, J., 'The importance of keeping your company's trade secrets, secret' available at https://www.ipcybersecurity.com/free-guide-1. Analysing the similarities between the EU TSD and U.S. trade secret law see Sandeen, S.K., 'Implementing the EU Trade Secrets Directive: a view from the United States' [2017] EIPR 4; and Wennakoski, A.A., 'Trade secrets under review: a comparative analysis of the protection of trade secrets in the EU and in the US' [2016] EIPR 154. On U.S. trade secret law more generally see Milgrim, R.M. & Bensen, Eric. E., *Milgrim on Trade Secrets* (Lexis Nexis); Pooley, J.A., *Trade Secrets* (Law Journal Press); and Rowe, E.A. & Sandeen, S.K., *Trade Secrets Law: Cases and Materials* 3rd ed (West Academic).

[119] See, for example, Drexl, 2018, pp. 93-106; Leistner, M., 'The existing European IP rights system and the data economy – An overview with particular focus on data access and portability' in Josef Drexl et al (eds), *Data Access, Consumer Protection and Public Welfare* (Nomos 2021), pp. 209-251, available at https://doi.org/10.5771/9783748924999, at pp. 232-235; Nordberg, 2020; and Sandeen, S.K. & Aplin,

Article 2(1) of the TSD defines "trade secret" as information which meets the following requirements:

> *"(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
>
> *(b) it has commercial value because it is secret;*
>
> *(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."*

Since the focus of protection is "information", this, as Drexl points out, *"clearly locates trade secrets protection on the semantic level of data"*.[120] In other words, it does not protect data on a syntactic level, i.e. the *"bits and bytes"*, but rather the information *encoded* in those signs, which itself has meaning.[121] The type of information that can be protected is broad and, as indicated by recital 14 TSD, includes technical information, know-how and business information. Provided the elements of secrecy, commercial value and reasonable steps are met, then there is nothing that *prima facie* precludes data (in the semantic sense) from being protected.[122] However, when it comes to satisfying the criteria for protection, this is where uncertainties arise. Thus, it is perhaps no surprise that industry participants expressed some confusion over whether the data they held was protectable as a trade secret. We turn first to consider the requirement of "commercial value", looking at its general interpretation, before considering how it relates particularly to data.

5.2.1 What is commercial value?

Article 2(1)(b) of the TSD requires the information to have *"commercial value because it is secret."* Recital 14 of the TSD elaborates upon the meaning of *"commercial value".* It indicates that it may be *"actual"* or *"potential".* Further, that:

> *"know-how or information should be considered to have a commercial value, for example, where its unlawful acquisition, use or disclosure is likely to harm the interests of the person lawfully controlling it, in that it undermines that person's scientific and technical potential, business or financial interests, strategic positions or ability to compete".*

In one sense, recital 14 describes what is *not* of commercial value by excluding trivial information. Further, recital 14 indicates that "value" may be assessed by the harm caused by trade secret misappropriation, where harm is conceptualised broadly as undermining various interests – whether they be technical, business, financial, or the ability to compete. In other words, the example is framed as *if* there was misappropriation (i.e., acquisition, use or disclosure of this information without permission), would the person lawfully controlling the trade secret be in a less competitive position, or lose money, custom, goodwill, etc. To put the question in its positive sense, it requires asking whether the information provides an *advantage* vis-à-vis its competitors. However, recital 14 overlooks a key element of the definition in Article 2(1)(b) TSD, namely, that there must be *commercial value because the information is secret* as opposed to commercial value *per*

T., 'Trade Secrecy, Factual Secrecy and the Hype Surrounding AI' in Abbott, R. (ed) *Research Handbook on Intellectual Property and Artificial Intelligence* (Edward Elgar, 2022), ch 24, pp. 442-459, available at SSRN: https://ssrn.com/abstract=3929928.

[120] Drexl, 2018, p. 92.

[121] See Drexl, 2017.

[122] Aplin, T., 'Trading Data in the Digital Economy: Trade Secrets Perspective' in Lohsse, S. Schulze, R. and Staudenmayer, D. (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (2017, Nomos), pp. 59-74 and Drexl, 2018, pp. 92-93 (referring to data collected through connected devices).

se. Thus, an interpretation of commercial value must include not just the competitive advantage bestowed by the information (or the harm caused if it were misappropriated), but the fact that this advantage (or harm) arises *because* the information is secret.

U.S. law has a similar concept – that of "independent economic value"[123] – which Hrdy has examined at length.[124] She explains that while this requirement has often been overlooked by courts, or treated as easily satisfied, there is now a trend to pay greater attention to it and, indeed, this will be important for developing federal jurisprudence on the Defend Trade Secrets Act 2016 (DTSA). Hrdy points to information that may struggle to satisfy the independent economic value criterion, such as: *"private information that is unrelated to business operations, routine internal documents; software incorporating significant amounts of open source (public) code; large compilations of data that contain significant quantities of public information; minor product modifications; undeveloped ideas without a plausible path to commercialization; and outdated technology whose commercial relevance has expired."*[125]

Hrdy also points to the importance of providing *direct evidence* of independent economic value, such as through revenues from licensing trade secrets or increased revenues from a trade secret being used in a product design.[126] Examples of where value did not arise from secrecy, include *Yield Dynamics*[127] and *Signal Financial Holdings.*[128]

In *Yield Dynamics,* the issue was whether eight segments of source code copied by a former employee had independent economic value. The plaintiff argued that the code, despite much of it deriving from public sources, was valuable because it would help a programmer save time. The trial court (upheld on appeal) found that the plaintiff had failed to provide any evidence of independent economic value. It was not enough *"[m]erely stating that information was helpful or useful to another person…or that information of that type may save someone time…[the court] is entitled to expect evidence which it can form some solid sense of how useful the information is, e.g., how much time, money, or labor it would save."*[129] Evidence that the plaintiff used NDAs did not suffice here either because it was the plaintiff's practice to keep *"all of its code confidential, even though some of it came from outside sources, including public ones."*[130] Finally, the court stated that *"the core inquiry is the value to the owner in keeping the information secret from persons who could exploit it to the relative disadvantage of the original owner*".[131] However, there was no evidence that the defendant's products competed with the plaintiff or its products.

Another example of where a trade secret was not established is *Signal Financial Holdings.* Here, it was held that draft employee agreements (that had been taken by a former employee) lacked independent economic value due to secrecy. While the templates were

[123] Section 1(4) of the UTSA, which has been adopted by 47 U.S. states and "has been the primary source of trade secret law in the United States": Sandeen, S.K. & Rowe, E.A., *Trade Secret Law* 2nd edition (West Academic Publishing, 2018). There is similar language in the U.S. Federal Defend Trade Secrets Act 2016 (DTSA) Public Law 114-153, May 11, 2016, which amended the Economic Espionage Act 1996 (EEA): see 18 U.S.C., chapter 90, § 1831, *et seq.*

[124] See Hrdy, C.A., 'The Value in Secrecy' (August 2, 2021). Available at https://ssrn.com/abstract=3897949 or http://dx.doi.org/10.2139/ssrn.3897949.

[125] Hrdy, 2021, p. 6.

[126] See the discussion of Hrdy, 2021, pp. 32-40.

[127] *Yield Dynamics, Inc., v. TEA Systems Corporation,* 154 Cal. App. 4th 547 (2007).

[128] Signal Financial Holdings LLC v. Looking Glass Fin. LLC, United States District Court, N.D. Illinois, Eastern Division, 2018 WL 636769.

[129] *Yield Dynamics,* pp. 564-5.

[130] *Yield Dynamics,* p. 566.

[131] *Yield Dynamics,* p. 568.

useful in creating future agreements (and thus reducing legal fees), the court commented *"that would be the case even if the documents were public"*.[132]

The lesson that can be taken from this U.S. jurisprudence for an EU setting is that, ideally, trade secrets holders should *show direct evidence* of value in the form of licensing trade secrets or increased revenues due to use of the trade secret. Also, circumstantial evidence of the investment in developing the secret information and keeping it secret will be relevant, but not necessarily determinative.

In the absence of CJEU rulings on the TSD, and a limited number of Member State national court decisions,[133] U.S. jurisprudence could be used as the basis for industry guidance on the meaning of "commercial value because of secrecy", more generally. When it comes to how this criterion applies to the data economy, however, U.S. jurisprudence does not provide specific answers. We turn now to consider some of the issues specific to the data economy.

Data economy considerations

When it comes to the data economy, questions of legal interpretation arise about whether trade secrets protection arises in relation to individual data versus datasets; machine-generated data; and training data for AI.

It is unlikely that individual data will have commercial value.[134] On its own, individual data (e.g., a particular measurement or reading of a connected device relating to fitness, health, utilities, or cars), is not useful or meaningful in isolation. As Drexl observes, the sensors on interconnected devices typically produce data that involve little semantic information. Further, Article 2(1)(a) of the TSD refers to secrecy of the information *"as a body or in the precise configuration and assembly of its components"* – in other words it assumes that information is in an aggregated or combined form rather than a single piece of information. Also, the purpose of the TSD is to stimulate innovation and knowledge sharing and it is hard to imagine how individual or isolated data would contribute to that aim. Rather, it is only when individual data are combined into individual-level datasets (e.g. all data generated by a particular connected device) or aggregated datasets (all data generated by a multiple of connected devices) that such value may arise.[135] In the case of individual level datasets generated from connected devices, Drexl has commented that access to such information by competitors does not necessarily destroy the competitive advantage of the manufacturer of the device, except where the data relates to the technical functioning of the device and helps the manufacturer to improve the device and provide maintenance services (i.e. when the raw data becomes derived or inferred data).[136] In the case of aggregated datasets, there are well-developed markets for non-personal data, relating, for example, to financial or commodities markets, credit scoring, weather, car matriculation data and geo-location data.[137] Where there exist specific markets for such diverse data, it may be possible to show that unlawful acquisition, use or disclosure of

[132] *Signal Financial Holdings LLC,* *5. By way of contrast, the slide deck that was used to pitch for investment funding was held to be a trade secret – the compilation of information had involved "considerable time and effort" to create and was valuable for acquiring investment funding, and third party access was regulated by a non-disclosure agreement.

[133] See De Vroey & Allaerts, 2021; Germany (2021) 52(6) IIC 775 and Poland (2020) 51(9) IIC 1129. See also *Shenzen Senior Technology Material Co Ltd v Celgard, LLC* [2020] EWCA Civ 1293, [28] (Arnold LJ).

[134] See Aplin, 2017 and Noto La Diega, G. & Sappa, C., 'The Internet of Things at the intersection of data protection and trade secrets. Non-conventional paths to counter data appropriation and empower consumers' (2020) 3 European Journal of Consumer Law 419, available at https://ssrn.com/abstract=3772700; Drexl, 2018, p. 93.

[135] See Noto La Diega & Sappa, 2020; Drexl, 2018, p. 93.

[136] Drexl, 2018, p. 94.

[137] European Commission, 'Staff Working Document on the free flow of data and emerging issues of the European data economy' SWD (2017) 2 final, p. 13; Mayer-Schönberger, V. & Cukier, K., *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray 2013), pp. 89–91.

aggregated datasets undermines the trade secret holder's business or financial interests, or its ability to compete. Even where markets for data do not yet exist, potential commercial value might nevertheless be established. However, it is important to ensure that such information has secrecy and commercial value because of that secrecy. It may be that data generated from connected devices (such as smart meters that track energy consumption), or that gleaned from public sources (e.g., public records to ascertain information about bankruptcy, judgment debts or tax liens or social media in relation to credit scoring) lacks secrecy,[138] and the aggregated version of this type of data will not change this status. Thus, while the data may have commercial value it will not be because of the secrecy of that information, as required by Article 2(1) of the TSD.

Another consideration is whether datasets used to train AI may be protected as trade secrets. To the extent that much of the data is drawn from public sources, this is unlikely to be the case.[139] Further, in instances where there is widespread availability of datasets, the secrecy requirement will not be met.[140] To the extent that there is investment in "labelling" the training data for supervised learning, the dataset is more likely to reach the level of commercial value.[141] But this does not mean that there is commercial value due to secrecy. If anything, the commercial value (i.e., competitive advantage) arises because the data can now be more effectively used. The same goes for where the dataset has been "cleaned" of redundant data. The output of AI training techniques will generate new information which may itself qualify as a trade secret if the necessary criteria are met, but the trade secret holder is likely to be the person who has generated the new information from its use of machine learning techniques, rather than the person who has provided the labelled or cleaned dataset.

Turning to the situation (raised in interviews) where data initially has no value but is shared with a third party who later uses this data with a breakthrough innovation to create revenue: would the initial data have "potential value" under the EU definition of trade secret? We argue that it would not, and that firms' perceptions are correct (namely, that this is confidential information, but not a trade secret). This is because, at the time of sharing, there is no potential value in the data – i.e., it does not seem that, at that moment, the data gives the firm a competitive advantage. It may also be questioned, even assuming there is potential value, whether the secrecy of the information confers value, or whether it is simply that the data is useful (regardless of secrecy).

When it comes to what qualifies as a trade secret in the data economy, it seems clear that individual data and raw (or unprocessed) machine-generated data will not be protected. Individual and aggregated datasets, however, are less straightforward if they are inferred or derived data and protection will depend on whether the data within is drawn from publicly or widely available sources or from restricted sources and whether the commercial value is causally connected to secrecy, as opposed to simply the usefulness of the data. These assessments of secrecy and commercial value will be context specific. Nevertheless, it is advisable for the EU Commission to consider offering non legally binding guidance (i.e.,

[138] Drexl, 2018, p. 94; Sandeen & Aplin, 2022.

[139] Sandeen & Aplin, 2022.

[140] Peng, K., Mathur, A. & Narayanan, A., 'Mitigating dataset harms requires stewardship: Lessons from 1000 papers' Draft paper 9 August 2021, available at https://openreview.net/forum?id=KGeAHDH4njY, traces how two popular face and person recognition datasets (DukeMTMC and MS-Celeb-1M) remain widely available even after retraction by their originators, which they call 'runaway data'.

[141] Labelling means the training data is labelled as to what it represents, which allows the supervised learning model to determine whether its prediction was right or wrong: see Drexl, J. & Hilty, R. et al., 'Technical Aspects of Artificial Intelligence: An Understanding from an Intellectual Property Law Perspective' (October 8, 2019). Max Planck Institute for Innovation & Competition Research Paper No. 19-13, available at SSRN: https://ssrn.com/abstract=3465577.

interpretative soft law)[142] on the applicability of trade secrets protection in the data economy ahead of any judicial clarification, which is likely to take some time to emerge.

5.2.2 Reasonable steps

The empirical data suggested a desire for clarity on the requirement of "reasonable steps" to maintain secrecy (see case study 4, for example, referring to "reasonable steps"). In determining what constitutes "reasonable steps", there are questions about whether the assessment will be subjective, according to the circumstances of the particular business involved and the cost of those measures to that business, or whether it will be objective, measured by the usual protective measures that are adopted in the sector. With only limited European jurisprudence so far,[143] we may turn to U.S. law for guidance. Professors Sandeen and Rowe[144] describe the purpose of the "reasonable steps" requirement in the UTSA and DTSA as one of *identification* of the trade secret and putting others on *notice* of the trade secret. They also note that reasonable steps may operate as circumstantial evidence of secrecy or economic value, but that it is important to keep the substantive requirement separate from its evidential function for the other limbs of the trade secret definition.

"Reasonable efforts", as it known in U.S. trade secrets law, requires a *"highly factual and contextual analysis"* and is treated as a question of fact.[145] The reasonable measures do not require absolute secrecy, but relative secrecy and there is a weighing up of the nature and value of the putative trade secrets and the cost of precautions to the putative trade secret holder. This suggests that the greater the value of the trade secret, the higher the standard of "reasonable measures" will be. It is clear that U.S. law takes a relative, contextual approach – i.e., analysing the type of trade secret in the context of the trade secret holder's business.[146] It is likely that national courts in EU Member States and the CJEU would adopt a similar approach,[147] although there may still be a low, objective threshold that needs to be met, regardless of the type of business. For example, if a business decides to share data, a baseline "reasonable step" could be to use a non-disclosure agreement to share and to include a term requiring the licensee to take reasonable steps to ensure the information remains secret. In the case of digitally stored data, a minimum reasonable step could be to use technological protection measures to control access to that data.

In terms of evidence of reasonable efforts, the guidance that can be gleaned from U.S. case law is that the following types of measures will be relevant: i) use of non-disclosure or confidentiality agreements; ii) restricting access to information; iii) measures taken in relation to employees and ex-employees (e.g., exit interviews and terminating access to information systems once left); iv) technological security measures; v) physical security measures; vi) identifying and labelling information as confidential or trade secrets.[148] Also,

[142] Pursuant to Art. 288 of the Treaty on the Functioning of the European Union. "Interpretative" soft law provides "guidance as to the interpretation and application of existing EU law": see Senden, L. *Soft Law in European Community Law* (Hart, 2004), p. 118.

[143] De Vroey & Allaerts, p. 1394 briefly discuss a few cases decided before the TSD was implemented that could be relevant to reasonable steps.

[144] *Trade Secret Law* 2nd edition (West Academic Publishing, 2018), pp. 93-94.

[145] Sandeen & Rowe, 2018, p. 94 citing *Rockwell Graphic Sys Inc v DEV Indus., Inc.,* 925 F. 2d 174, 176-77 (7th Cir. 1991).

[146] Sandeen & Rowe, 2018, p. 100: "The inquiry necessarily varies in each case based on the costs of the protective measures relative to the risks of misappropriation and the attendant benefits of protecting the information".

[147] For example, Angsar Ohly discusses how "reasonableness" is a "flexible, malleable and relative concept" and how the German government has provided basic criteria of the absolute value of the trade secret, its relative value to the trade secret holder and the costs and availability of protection measures: see Ohly, A., 'Germany: The Trade Secrets Protection Act of 2019' in Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonisation and Protection of Trade Secrets in the EU* (Edward Elgar, 2020), ch 7, pp. 104-124, at p. 109.

[148] See Sandeen & Rowe, 2018, 101 and Beale & McFarlane.

the size of the organisation may impact what constitutes "reasonable steps"[149] and its level of sophistication may affect whether such steps are taken.[150]

The above are indicative examples of "reasonable steps" for all types of information; however, they may be usefully adopted as guidance by firms working with confidential and commercially valuable data. Indeed, the empirical data in this study suggests that many of these types of steps are already being taken (see case study 11, for example). What will be required is for firms to *differentiate* between the relative value of their trade secrets and to use stronger protections for their most valuable information. While the empirical data suggests that different measures are already being taken depending on the value of the confidential and commercially valuable data, this is not happening across the board. Therefore, it would be advisable for the EU Commission to consider issuing guidance (in the form of interpretative soft law) about the range of "reasonable steps" that may be taken and for specific workshops to be held to encourage industry dialogue about the practices that they routinely adopt in relation to their data.

5.3 Employees/ ex-employees

The empirical data revealed that a significant concern for companies is trade secret leakage through employees or former employees. This is a concern both for the trade secret holder (i.e., the former employer) and the new employer, who might inadvertently access and misuse a trade secret that has been *"carried over by new staff from the previous employer"* (see section 3.2.4). Managerial processes - at the hiring, training and departure stages of an employee's employment - were therefore seen as key by some interview partners, and guidance about what these might entail, in particular to satisfy the "reasonable steps" requirement for trade secret protection, was noted in Case study 4.

It is suggested that the following measures would be important to preserving the secrecy of CCV data or know-how (i.e., satisfying the "reasonable steps" requirement) and ensuring that companies do not end up accidentally misappropriating trade secrets. At the hiring stage, companies should identify what confidential and commercially valuable data or know-how the new employee is bringing with her and ensure that confidentiality obligations or non-compete clauses are inserted into the employment contract. At the training stage, companies should ensure that staff are aware of the appropriate technical and legal security measures for accessing and sharing data (e.g., only sharing information where NDAs are signed or restricted access to certain groups of people). Finally, at the departure stage, companies should hold exit interviews to reiterate any legal obligations regarding confidentiality or non-competition and clarify what should not be copied or taken with them; and ensure that there is no longer continued access to the physical or IT infrastructure that would enable access to CCV data. The Commission may want to consider whether it is worthwhile to provide guidance on these matters to EU companies (such as through interpretative soft law or FAQs on its website) and whether to facilitate workshops whereby companies can share their good practice about such managerial processes. This may be particularly relevant for SMEs.

As discussed in section 3.1.1 above, the TSD does not provide much of a legal framework for governing employees and ex-employees. This is mainly left to Member States' laws.[151] There are only a few provisions in the TSD that *explicitly* address employees. These are

[149] See *Puroon Inc. v Midwest Photographic Res Ctr Inc.,* 2018 WL 5776334 (N.D. Ill. Nov 2, 2018) and *Elmer Miller Inc. v Landis,* 253 Ill. App. 3d 129 (1st Dist. 1993).

[150] Our interview with a U.S. legal expert suggested that U.S. companies either take a sophisticated approach to trade secrets, categorising their information and tailoring their protection measures accordingly; or they take a crude approach of lumping all information together and regularly using NDAs in relation to sharing such information; or they take few measures.

[151] For a discussion see Domeij, B., 'The Trade Secrets Directive and employees' in Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonisation and Protection of Trade Secrets in the EU* (Edward Elgar, 2020), ch 9, pp. 151-172.

Articles 1(3) and 14(1) and recitals 13, 14 and 30 of the Directive. In essence, these provisions seek to ensure that Member States continue to have considerable freedom in how they regulate employees and ex-employees via express and implied contractual duties.[152]

What is clearly preserved to the discretion of Member States is the possibility of remedial limitations for employees. Article 14(1) of TSD states "Member States may limit the liability for damages of employees towards their employers for the unlawful acquisition, use or disclosure of a trade secret of the employer where they act without intent". Recital 30 echoes this provision.[153] This would allow, for example, the Swedish approach to damages (see Art 7 of the Sweden Law on Trade Secrets 2018:558) to continue.

Also preserved is the autonomy of Member States to regulate employees and ex-employees through contract, including through non-compete clauses. This much is acknowledged in Article 1(3)I, which states that the Directive does not impose, in relation to employee mobility, "any additional restrictions on employees in their employment contracts *other than restrictions imposed in accordance with Union or national law*". The italicised language makes clear that any restrictions on mobility *can* come from national law. This is reinforced by recital 13, which states that the TSD is not *"intended to affect the possibility of concluding non-competition agreements between employers and employees, in accordance with the applicable law"*. As such, how former employees are regulated and the principles regulating non-compete clauses or agreements are left to Member States.

The TSD is also at pains to ensure that its provisions are not misconstrued as affecting employee mobility, leaving this important area to be regulated at Member State level.[154] For example, Article 1(3) states that "*Nothing in this Directive shall be understood to offer any ground for restricting the mobility of employees…"* or as "limiting employees' use of information that does not constitute a trade secret" or *"limiting employees' use of experience and skills honestly acquired in the normal course of employment"*.[155]

The TSD does, however, indirectly overlap with Member States' approaches to employees/ex-employees. This is because employees may fall foul of unlawful acquisition of a trade secret, as defined in Article 4(2).[156] Further, Article 4(3)(b) and (c) TSD defines unauthorised use or disclosure as including *"breach of a confidentiality agreement or any other duty not to disclose the trade secret" or "breach of a contractual or any other duty to limit the use of the trade secret".* Thus, to the extent that employees or ex-employees are in breach of any confidentiality obligations or loyalty obligations or non-compete clauses (which themselves will be regulated by Member States' laws), use or disclosure of a trade secret will be unlawful according to the TSD. Recital 14 also indicates that the "experience and skills gained by employees in the normal course of their employment" is not a trade secret. This does create an issue of potential interpretation for the CJEU, which is whether *"experience and skills gained by employees"* is a matter of EU law or not, or whether it should be left to national law. In either case, it seems that differentiating between what is in an employee's general skill and experience and what is not (and thus potentially a trade secret) is inherently difficult.[157]

[152] See Kolasa, M., *Trade Secrets and Employee Mobility: In Search of an Equilibrium* (CUP, 2018), p. 156.

[153] Recital 30 TSD states that Member States may provide "in their national law that the liability for damages of employees is restricted in cases where they have acted without intent".

[154] For a discussion of this complex area, where there are divergences between Member States see Kolasa, 2018 and Van Caenegem, W., *Trade Secrets and Intellectual Property: Breach of Confidence, Misappropriation and Unfair Competition* (Wolters Kluwer, 2014).

[155] This latter point is also emphasised by recital 14.

[156] Discussed by Domeij, 2020, pp. 159-160.

[157] Domeij, 2020, pp. 154-155.

Because the TSD does not significantly harmonise the regulation of employees and ex-employees and leaves considerable autonomy to Member States, this means that companies will need to navigate the complexity of, and variations between, different Member States' laws, particularly when it comes to confidentiality and non-compete obligations. This is particularly relevant to cross-border sharing of know-how and data and companies that have employees in multiple Member States. Interestingly, nothing emerged in the empirical data that pointed to such divergences being problematic in practice. Nevertheless, when it comes to innovation more generally, and the data economy in particular, it is advisable for the EU Commission to monitor whether such divergences in regulation of employees and ex-employees are creating a barrier to innovation or cross-border sharing of data such that greater legal harmonisation is needed.

5.4 The relationship of contract and trade secrets law

The empirical data (e.g., case studies 4, 8, 10, 12, 13 and the results of the survey) revealed that contractual means are routinely used for protecting confidential and commercially valuable data. Further, the data suggests that for many industry participants contractual measures are both *essential* and *prevalent* because they can be tailored to determine access/sharing and the obligations of how to handle data. In some instances, however, other forms of legal protection are seen as important complementary forms of protection, such as trade secrets and *sui generis* database protection.

The TSD is unlikely to disrupt the influential role of contractual agreements when it comes to data management and sharing, for several reasons. First, the TSD assumes that the protection it creates is in addition to that available under contract law. While the TSD is agnostic about the legal means of implementation (provided it does not create a property right), contract law would not suffice fully to implement the obligations in the Directive. Therefore, it is clear that contract sits alongside the TSD obligations. Second, use of contractual measures, such as NDAs or confidentiality obligations on employees, are crucial for helping to establish the "reasonable steps" requirement for protection as a trade secret under Article 2(1) of the TSD. Third, contractual obligations are a key means for determining when there is unlawful acquisition, use or disclosure of a trade secret under Article 4 TSD. As such, contractual protection reinforces elements of EU trade secrets law.

There are other issues that arise when it comes to the relationship between trade secrets and contract law. The first is the extent to which contractual measures can legitimately undermine or circumscribe lawful acts under Article 3 of the TSD. Second, we must consider the extent to which contract leads to "overclaiming" of trade secrets protection or excessive protection.

Turning first to the issue of contractual override of lawful acts in Article 3, TSD, this arises in the case of reverse engineering in Article 3(1)(b). This provision states that trade secret acquisition *"shall be considered lawful when the trade secret is obtained by…(b) observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret".* In cases of lawfully in the possession of the acquirer of the information, there must be no legally valid duty to limit the acquisition of the trade secret. Recital 16 of the TSD elaborates on this requirement, indicating that: *"Reverse engineering of a lawfully acquired product should be considered as a lawful means of acquiring information, except when otherwise contractually agreed. The freedom to enter into such contractual arrangements can, however, be limited by law."* (emphasis supplied)

Although recital 16 suggests that there could be contractual override of *all* lawful acquisition by reverse engineering, when read together with Article 3(1)(b) it seems clear that this is directed to instances where a person is in lawful possession of a product. In other words, it appears that agreements to hire, rent or license products *could* contain a provision that precludes study or disassembly for the purposes of reverse engineering. However, it is possible for Member States to limit the freedom to enter into such contractual arrangements. The same does not appear to be the case for contracts of sale and, by implication, this suggests that it is not possible contractually to override reverse engineering of products purchased on the open market.[158] To give an example, a purchaser of an autonomous vehicle could legitimately pull it apart to understand how the vehicle operates (in terms of physical and IT engineering) without this constituting unlawful acquisition of a trade secret. However, to the extent that an autonomous vehicle is rented or hired by a third-party organisation, the manufacturer of the vehicles could prohibit those third parties from any kind of disassembly or study of the vehicle that enables it to understand its functioning.

From a normative perspective, contractual restrictions on lawful acquisition by reverse engineering are problematic, at least where the product is software, because this creates an inconsistency with copyright law, which makes the reverse engineering and decompilation exceptions imperative as a matter of EU law.[159] The empirical data did not suggest that contractual restrictions on reverse engineering of lawfully acquired products were regularly in use, or, if they were in use, were currently having a deleterious effect on access to, or sharing of, know-how or data. However, it would be advisable for the EU commission to monitor this situation, particularly since Member States may take different approaches to whether contractual override of reverse engineering in the case of lawful possession of a product is permissible.

Another issue is the extent to which contract may contribute to "overclaiming" of trade secrets protection. To understand this, we must appreciate that those who factually have control over data can assert "ownership" of the data as a trade secret when it comes to contractual agreements. While there are objective requirements under Article 2(1) of the TSD, these are not assessed *ex ante,* as occurs with registered IP rights, such as patents. Therefore, it is possible for a data holder to assert trade secrets in a licensing agreement or non-disclosure agreement, even where the data is not secret, lacks independent economic value or has not been subject to reasonable steps for protection. In other words, contract allows factual secrecy – as opposed to trade secrecy – to be preserved and monetised.

Several observations can be made about this tendency. The first is that the uncertainty about whether the objective criteria of "trade secret" are satisfied in the context of the data economy (in conjunction with the lack of *ex ante* assessment) contributes to the tendency to assert trade secret "ownership" of data in contractual arrangements. Second, to the extent that the data is *not* a trade secret, this will mean that "ownership" can only be effectively enforced between the contractual parties – it will not be possible to enforce the protection in the TSD against third parties. However, this fact may not preclude a data holder from asserting trade secrets protection, which can only, ultimately, be tested by litigation. This creates a risk of third parties being sued for trade secret misuse (even if the courts do not ultimately uphold the claim), which in turn may generate more conservative behaviour on the part of third parties when it comes to data sharing. Thus, it is important that the application of the TSD to the data economy is clarified, either by the legislature or the courts.[160] While judicial interpretation has the advantage of flexibility and a context-sensitive approach, it may take considerable time to develop jurisprudence (as seen in the case of Japan, discussed below). Therefore, in the light of potential negative impacts of "overclaiming" trade secrets protection when it comes to the data economy, at the very least, non-legally binding guidance should be issued by the EU Commission about the application of trade secrets protection.

[158] See also Ohly, 2020, pp. 115-116.

[159] See Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) OJ L 111, 5.5.2009, pp. 16–22*,* Art 8: 'Any contractual provisions contrary to Article 6 or to the exceptions provided for in Article 5(2) and (3) shall be null and void'. C-406/10 *SAS Institute Inc v World Programming Ltd* ECLI:EU:C:2012:259, [2012] 3 CMLR 4; [2012] ECDR 22, [47]-[62] on the relationship between article 5(3) and article 8 of Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs OJ 1991 L 122, p. 42.

[160] See further the comments of Prof. Drexl in his peer review of the Report.

The use of contract to regulate access to information – even where it may not satisfy the requirements of Article 2(1) TSD – also means that the checks and balances of trade secret law, particularly in Articles 3 and 5 – can be circumvented.[161] More attention therefore needs to be paid to whether those checks and balances should be applicable to factually secret data that does not reach the threshold of "trade secret". It would be advisable for the EU Commission to investigate further this policy issue.

5.5 Other observations about the Trade Secrets Directive

Our legal experts observed that the TSD, as compared with trade secrets protection in the U.S. and Japan, seemed nuanced and balanced because of the limitations in Articles 3 and 5[162] of the TSD, the emphasis on proportionality when it comes to enforcement and remedies (in Articles 11 and 13, TSD), and the introduction of an obligation to preserve confidentiality during legal proceedings (in Article 9, TSD). These are laudable aspects of the TSD that have contributed to its support in the literature.[163]

5.6 The position in Japan – "shared data with limited access" protection plus lessons re "trade secrets"

To the extent that trade secrets protection may not be available for machine-generated data (because there are difficulties with satisfying the definition of "trade secret"), the introduction of protection for "shared data with limited access" in Japan may be of interest to EU policymakers. In 2018, changes were introduced to the Unfair Competition Prevention Act (Act No 47 of 1993, revised in 2018) (UCPA) of Japan. Specifically, in order to incentivise commercialisation of "big data", such as map data, weather data, machine generated data and consumption trend data, legal changes to Japanese unfair competition law were introduced to prevent unauthorised acquisition, use and disclosure of "shared data with limited access".[164] As indicated in our interviews with legal experts, this added protection was thought to be necessary because of the uncertainty about whether machine generated data would qualify as a trade secret and given the absence of a *sui generis* database right, as exists in the EU. There was also considerable support for this proposal from key industry stakeholders, particularly from the automotive industry.

Article 2(7) of the UCPA defines "shared data with limited access" to mean *"technical or business information that is accumulated to a significant extent and is managed by electronic or magnetic means…as information to be provided to specific persons on a regular basis (excluding information that is kept secret)"*. *"Technical or business information"* is meant to include machine generated data, datasets for AI software, as well as *"consumption trend data"* and *"market research data"*.[165] The requirement of significant accumulation is meant to signal that the focus is on big data and similar information and electromagnetic management (e.g. through authentication or encryption) is meant to

[161] In much the same way as occurred in Case C-30/14 *Ryanair Ltd v PR Aviation BV,* ECLI:EU:C:2015:10 and critiqued by Borghi, M. & Karapapa, S., 'Contractual restrictions on lawful use of information: sole-source databases protected by the back door?' [2015] EIPR 505.

[162] Discussing these limitations see Aplin, 2021 and Mylly, 2021.

[163] See Schovsbo, J., 'The Directive on trade secrets and its background' in Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar, 2020), ch 2, pp. 7-21, describing the TSD as providing "EU Member States with a boilerplate for their national protection…which should allow national legislators and courts to arrive at a harmonious result" (p. 21). See also Leistner, 2021 describing the TSD as "modern, balanced and proportional protection" and as "rather well equipped to contribute a flexible protection instrument to the regulation of the data economy" (pp. 234, 235).

[164] Ministry of Economy, Trade and Industry, *Guidelines on Shared Data with Limited Access,* 23 January 2019, available at https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines_on_shared_data_with_limited_access.pdf (Guidelines).

[165] Guidelines, p. 10.

signal the *"intention to control data"*.[166] Notably, *"shared data with limited access" excludes* trade secrets (based on the language *"excluding information that is kept secret"* in Art 2(7) UCPA) and *"open data"* (based on Article 19(1)(b) UCPA "any information that has been made available to the public without compensation"). Information can be classified as *not* being kept secret, even where access control measures are used. What seems to be key is that there is an intention to share the data.[167] In terms of "open data" this is where data is provided *gratis* to a wide range of users without restriction.[168] While, theoretically, there seem to be clear distinctions between these three categories of information, it remains to be seen whether this is the case and whether these are understood by industry. In speaking with our Japan experts and looking at the literature, it was not apparent that industry had raised any difficulties with this new form of protection or the Guidelines accompanying it.

The revised UCPA creates protection against unauthorised acquisition, use or disclosure of shared data with limited access.[169] Unfair competition, rather than a property type, protection was chosen, in order to ensure a balance between holders, and users, of shared data.[170] For a person who has no right to access the shared data, they may wrongfully acquire the data through theft, fraud, duress or other wrongful means, and any use or disclosure of shared data wrongfully acquired is prohibited. For a person who has the right to access the shared data, it is prohibited to use or disclose the shared data, in violation of the duties regarding management of that data, for the purpose of wrongful gain or causing damage to the holder of shared data with limited access. There may well be complexities in ascertaining whether the relevant act of use or disclosure is permitted by the holder of shared data with limited access.[171] Finally, a prohibition extends to subsequent acquisition, use or disclosure in bad faith at the time of acquisition (see Art 2(xii), (xv)). This requires knowledge that there has been an *intervening (i.e., earlier) act* of either wrongful acquisition or improper disclosure, or knowledge that the disclosure of that data is an act of improper disclosure. Further, that you are dealing with the same data.[172] Knowledge here seems to refer to actual, as opposed to constructive, knowledge (unlike trade secrets protection).[173] Where there is good faith acquisition but subsequent notice that there were wrongful acts, a person will only be liable for a remedy where the acts of disclosure may spread, causing consideration damage to the holder (Art 2(1)(xiii) and (xvi)).

The Ministry of Economy, Trade and Industry has produced detailed Guidelines[174] on the new type of unfair competition protection for shared data with limited access. The reception to these Guidelines appears to have been neutral. No case law has emerged in relation to "shared data with limited access" protection. Whether the new form of protection, and the Guidance provided, has enabled business greater confidence in sharing their data is yet to be seen. Certainly, from our interviews with Japan experts, there was a sense that existing trade secrets law and contract law were sufficient to protect data in the data economy and that this new type of protection in Japan was not empirically shown to be necessary or to have yet had a positive impact. Rather, the new type of protection was "performative" – policymakers being seen to be doing something to promote the data economy. The view

[166] Guidelines, pp. 7 and 8.

[167] Guidelines, p. 12.

[168] Guidelines, p. 13.

[169] See Art. 2(1)(xi)-(xvi).

[170] Guidelines, p. 16. The wisdom of rejecting property-type protection in data is explained by Drexl, 2017.

[171] See the discussion in Guidelines, pp. 25-33.

[172] Guidelines, pp. 39-40.

[173] Guidelines, p. 42 states that there is no liability where lack of knowledge is due to gross negligence. "For shared data with limited access, therefore, the subsequent acquirer is not obligated to verify or investigate whether wrongful conduct has occurred".

[174] Ministry of Economy, Trade and Industry, *Guidelines on Shared Data with Limited Access,* 23 January 2019, available at https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines_on_shared_data_with_limited_access.pdf (Guidelines).

was also expressed that, if additional or specialised protection was shown to be needed, then this type of unfair competition type scheme for "shared data with limited access" is preferable to a property right scheme.[175]

Our recommendation is that the EU should not introduce a type of Japanese "shared data with limited access" right, but instead should monitor, with interest, the impact of this model of protection in Japan. This is for several reasons. The first is that this right was developed within a specific legal context, where the absence of a *sui generis* database right and the scope of protection under trade secrets law were perceived to be problematic. In the EU, there is, of course, a *sui generis* database right, even though there have been qualifications (and proposed qualifications) to this right in order to promote the data economy.[176] Second, the Japanese scheme applies to *any* data that is shared and therefore provides far-reaching protection for data that might have an inhibiting effect on data-sharing or accessing data. Further, any such scheme would cause difficulties with coordinating data access and data use rights.[177] Finally, the Japanese scheme is relatively new, and its positive impact on data sharing is, as yet, unproven. The EU should therefore hesitate to introduce a new form of protection, without clear evidence of how this will be beneficial to the data economy.

Some interesting, general observations about trade secrets protection emerged from our interviews with Japan experts. The first is that the jurisprudence on what constitutes a "trade secret" took a couple of decades to settle from the time protection was first introduced in the UCPA in 1990 to the present day.[178] Alongside this, the Ministry of Economy, Trade and Industry produced "Management Guidelines for Trade Secrets" that have been periodically revised,[179] in response to case law developments and industry feedback. This experience suggests that, in an EU context, it will take time for a legal and business understanding of "trade secret" to develop. Thus, in the meantime, it would be wise for the EU Commission to issue soft law guidance in relation to the TSD – in particular, the scope of the definition of "trade secret" as it relates to data – while at the same time leaving it to national courts and the CJEU to interpret.

Second, our Japan experts noted the role that criminal sanctions appeared to play with trade secrets protection. They commented that the repeated increase in criminal penalties had been at the instigation of business and that there was a preference to enforce via criminal prosecutions for cost-saving reasons. There had been 23 decisions by district courts in Japan between 2009 and 2020, largely concerning high-profile cases of industrial espionage or clear misuse by former employees and, due to their wide reporting in the media, this was likely to have a deterrent effect. By way of contrast, as the TSD does not harmonise criminal measures, there remain substantial divergences in criminal penalties between Member States. While there should be considerable caution in relation to criminal sanctions for trade secrets misuse because of the potential chilling effect on legitimate activities, it would be valuable for the Commission to explore whether harmonised *limits* on criminal penalties would be beneficial.

[175] This view is echoed by Leistner, 2021, p. 248.

[176] See Directive (EU) 2019/1024 on open data and the re-use of public sector information of 20 June 2019, OJ 2019 L172, Art 1(6) preventing public sector bodies from relying on the *sui generis* database right to prevent or restrict the re-use of public sector documents. See also the Data Act Proposal (https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data), rec. 84 and Art. 35 which state that the database right does not apply to databases containing data obtained from or generated by use of connected devices and related services.

[177] A point raised by Prof. Drexl in his peer review of this Report.

[178] See Suzuki, M., 'Japan' in Kung-Chung Liu & Reto Hilty (eds), *Trade Secret Protection: Asia at the Crossroads* (Kluwer, 2021), ch 1.

[179] Ministry of Economy, Trade and Industry, *Management Guidelines for Trade Secrets*, available at https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/0813mgtc.pdf.

Finally, our Japan experts contrasted the "infringing goods" provision in Article 4(5) of the TSD with Article 2.1(x) of the UCPA (introduced in 2015), which refers to "things created by the unlawful use of technical secrets". This notion is narrower than that of "infringing goods" in the TSD, because it is limited to goods resulting from the use of "technical secrets". While the intention to link the causality of "use" of a trade secret more directly with the resulting product may be seen as positive, our Japan experts noted that there are also uncertainties with Article 2.1(x), namely, whether "things" includes intangible products (such as software), what does "created by" mean and whether products made using trade secrets that are now no longer secret would be caught. What our discussion with Japan experts highlighted was the importance of ensuring that any "infringing goods" provision is narrowly delineated to ensure balanced protection. Drexl has also pointed out that the reach of the infringing goods provision in the TSD is broad and may apply to digital products and new information that is generated by data analytics in the data economy, although the knowledge requirement of the provision may have a constraining influence on its application in these situations.[180] It is recommended that the EU Commission revisits the drafting of Article 4(5) of the TSD to see whether a more balanced approach can be achieved.[181]

5.7 Data Act Proposal

The recently released Data Act Proposal[182] contains provisions dealing with the interface between data access/reuse and trade secrets and thus requires consideration here.

Overall, the aim of the Data Act is to ensure *"fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data"*.[183] More particularly, the Data Act, via the use of a Regulation, seeks to confer on users of connected devices the right to gain access to the data generated by these devices and to share such data with third parties.[184] As well, there are obligations on making data available to public sector bodies in cases of exceptional need.[185] Early scholarly evaluations of the Data Act have raised several concerns about its effectiveness.[186] It is beyond the scope of this Study to consider the Data Act in detail;[187] however, we do comment specifically on the interaction between trade secrets and the Data Act.[188]

Article 4(1) of the Data Act places an obligation on a data holder to make available to the user the data generated by the user's use of a product or related service (where this cannot be directly accessed by the user). Article 5(1) obligates a data holder to make data generated by the use of a product or related service available to a third party acting on behalf of a user. Further, Article 14(1) stipulates that, in cases of exceptional need (as defined in Article 15), data holders should make data available to public sector bodies and EU institutions, agencies or bodies. In each of these instances, obligations are created in

[180] Drexl, 2018, pp. 98-99.

[181] For a critique of Art. 4(5) TSD see Aplin, 2014, pp. 267-269 and Lee, 2020, p. 294.

[182] https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data

[183] Explanatory Memorandum, p. 2.

[184] Arts. 4 and 5, Data Act.

[185] Art. 14 Data Act.

[186] See Drexl, J., Banda, C., González Otero, B., Hoffmann, J., Kim, D., Kulhari, S., Moscon, V., Richter, H. & Widemann, K., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act) (2022), available at https://www.ip.mpg.de/en/research/research-news/position-statement-on-the-eu-data-act.html; and Kerber, W., 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (April 08, 2022), available at https://ssrn.com/abstract=4080436 or http://dx.doi.org/10.2139/ssrn.4080436.

[187] This has already been done in substantial and careful detail by Drexl et al (2022).

[188] This is also dealt with by Drexl et al (2022), [277]-[290].

respect of trade secrets – what we might describe as the "interface" provisions. Article 4(3) states that "*Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties."* Article 5(8) emphasises that *"Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party"* and that *"all specific necessary measures"* are taken *"to preserve the confidentiality of the trade secret"*. Further, Article 17(2)(c) indicates that where a public sector body makes a request for data under Article 14 then the request must *"respect the legitimate aims of the data holder, taking into account the protection of trade secrets and the cost and effort required to make the data available".* Further, Article 19(1) states that *"Disclosure of trade secrets or alleged trade secrets to a public sector body or to a Union institution, agency or body shall only be required to the extent that it is strictly necessary to achieve the purpose of the request."* And that body must *"take appropriate measures to preserve the confidentiality of those trade secrets".*

Before turning to the nature of these "interface" provisions, it is important to assess whether there will, in fact, be a clash between mandated data access and trade secrets protection. This depends, of course, on what data is required to be made available and it seems, according to recital 14 of the Data Act, that the Regulation will only apply to raw data generated or collected by connected devices, and *not* derived or inferred data.[189] However, raw data from connected devices is unlikely to qualify as a trade secret either because it lacks semantic meaning, or commercial value due to secrecy or secrecy (where it is exchanged on large data sharing platforms).[190] Whereas, it is only when the raw data is processed to produce derived or inferred data, or aggregated into larger datasets, that commercial value will occur and, even in those instances, the competitive advantage must arise from the secrecy of the data. Thus, it appears that the data access obligations in the Data Act should not clash with the trade secrets interests of data holders. If this is the case, then it is hard to see what role Articles 4(3), 5(8), 17(2)(c) and 19(1) – i.e., the "interface" provisions – would have to play.

However, it has been remarked that the fact that the Data Act is limited to raw data of the user (even if this can be a mixture of personal and non-personal data, and dynamic in nature) is highly problematic to achieving its aims.[191] As such, it has been recommended that the Regulation be amended to include inferred and derived data, and even the aggregated dataset of multiple users.[192] If this were the case then the provisions in Articles 4(3), 5(8), 17(2)(c) and 19(1) *would* come into play. Another situation that might trigger these "interface" provisions being relied upon is where data holders assert that their data is protected by trade secrets (even if this assertion is misplaced or an instance of "overclaiming").[193] Issuing soft law guidance on the applicability of the trade secrets definition in a data economy would therefore be helpful. Alternatively, the recitals to the Data Act could indicate the type of data that would *not* attract trade secrets protection. While such measures would not safeguard against deliberate "overclaiming" of trade

[189] *"Physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation…The data represent the digitalisation of user actions and events and should accordingly be accessible to the user, while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation."* (rec. 14)

[190] Drexl, 2018, p. 94.

[191] See Kerber, 2022, pp. 11 and 12, referring to the covered data as too "narrow" to enable third parties "to offer additional services to the users like repair or predictive maintenance services on downstream or adjacent markets".

[192] Kerber, 2022, p. 12.

[193] See also Drexl et al (2022), [281].

secrets protection, they might reduce the likelihood of doing so where "overclaiming" results from uncertainty or confusion about the scope of the law.

Assuming, therefore, that a clash between data access and trade secrets arises, the Data Act seeks to reconcile this in the case of users by requiring (in Article 4(3)) that *"specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties"*. The data holder and user can agree these measures. Yet, it is unlikely that such measures will be "agreed" as opposed to simply imposed by the data holder because they are in a better bargaining position. There is also uncertainty as to the extent of these measures, which might relate to technical protection measures (TPMs), other physical measures or NDAs, for example.

In the case of third parties (referred to Article 5) and public sector bodies (as defined in Article 2(9)), the same obligation applies ("necessary measures" for third parties and "appropriate measures" for public sector bodies), but there is an added requirement for third parties that disclosure of the trade secret is *"strictly necessary to fulfil the purpose agreed between the user and third party"* (Article 5(8)) and, in the case of public sector bodies, to the purpose of the request, i.e. the instance of exceptional need that has been identified (public emergencies or instances of public interest – see Article 15). While the purpose in relation to public sector bodies is framed reasonably clearly in Article 15, the "purpose" agreed between the user and third party referred to in Article 5(8) is stated in general terms. The intention behind the Data Act appears to be to promote aftermarket services for interconnected products;[194] however, recital 28 also refers to "development of entirely novel services making use of the data". As a result, the mandate to disclose the data to a third party could apply for *any* purpose that is agreed between the third party and the user of the interconnected device, and this could present a much greater threat to the trade secrecy interests of the data holder than if it was simply for the purpose of aftermarket services.[195] Therefore, it would be worth clarifying that the purpose *is* intended to be limited to aftermarket services for interconnected devices.

It is also unclear who is responsible for assessing whether trade secret disclosure is "strictly necessary" for the "agreed" purpose (in the case of third parties). Will it be the data holder? Or the requesting party? Or must it be via agreement? In each of these situations, there is a risk that the data holder could simply refute the necessity of the data for the relevant purpose and refuse to provide data on this basis, and this would undermine the effectiveness of the scheme. The recourse for parties in such a situation would appear to be via the enforcement mechanism in the Data Act, Chapter IX, although this does not preclude other administrative or judicial remedies.[196] Article 31 envisages that competent authorities will be appointed in each Member State,[197] and their responsibilities will include "conducting investigations into matters that concern the application of the Regulation" and "handling complaints arising from alleged violations of this Regulation".[198] Competent authorities are obliged to resolve complaints without "undue delay" and Member States must provide for "effective, proportionate and dissuasive" measures for infringements of the Regulation.[199] There is clear scope in this scheme for national variations in how enforcement occurs across the EU[200] and this could be problematic when it comes to disputes that arise in relation to cross-border data sharing. Moreover, if the mechanism for resolving complaints is not timely and it takes significant time to assess the necessity

[194] See Explanatory Memorandum and recitals 3 and 28 of Data Act.

[195] See also Drexl et al (2022), [288].

[196] Art. 32(1) Data Act.

[197] These may be existing authorities or newly established ones.

[198] Art. 31(3) Data Act.

[199] Art. 32(3) and Art. 33(1) Data Act.

[200] This is despite the obligation for competent authorities to cooperate across Member States "to ensure the consistent application of this Regulation": Art. 31(3)(f) Data Act.

of the information for the "agreed" or "requested" purpose, then the opportunity usefully to make use of this information may recede.

In the case of public sector bodies, the issue arises whether trade secret disclosure is "strictly necessary" for the "requested" purpose and how this is to be assessed. Here, the provisions seem (at least initially) presumptively to favour the public sector body, because Article 14 creates an obligation to provide data upon request and, according to Article 18, without delay, and Article 17(1) indicates what the public sector body needs to articulate in this request by way of justification. However, Article 18(2) envisages that the data holder may decline (or seek modification of the request) on the basis, *inter alia,* that the conditions of Article 17(1) (which includes demonstrating the exceptional need) are not met. As such, the data holder could, it seems, refute the basis of the request or whether the data are strictly necessary for this purpose and thus refuse to provide the data. Again, whether the enforcement mechanism envisaged by the Data Act will adequately resolve such disputes may be queried.

Turning to the measures that must be taken to protect confidentiality of the trade secret where the data *is* provided, in the case of third parties, all "specific necessary measures agreed between the data holder and the third party" must be taken by the third party. Again, there is a risk that there is no genuine agreement and it will be a matter of the data holder – who is in the better bargaining position – simply imposing the measures that will need to be taken, regardless of how onerous these might be for the third party. While a complaint could be raised through the envisaged complaint mechanism, there are issues about the effectiveness of this system (as already discussed above).

In relation to public sector bodies, the language of "appropriate measures" is used (in Article 19(1)) instead of "necessary measures" and it is unclear whether this is meant to indicate that less onerous measures need to be taken, bearing in mind the "public" status of a public sector body. Further, it does not seem that these "appropriate measures" need to be agreed but simply that the public sector body adopts them. On the other hand, the data holder can decline the request, *inter alia,* if Article 17(2) is not complied with and this includes respecting "the legitimate aims of the data holder, taking into account the protection of trade secrets". Thus, either there will be uncertainty on the part of the public sector body about the "appropriateness" of measures to protect confidentiality, or the data holder will, in reality, impose what these are.

Another issue that arises is whether users, third parties or public sector bodies would need to pay a fee for use of the data that is provided upon their request. Article 4(1) refers to the data being made available to users "free of charge" and in Article 5(1) to third parties "free of charge to the user". This suggests that users would not pay a fee, however, this does not preclude charges to third parties or public sector bodies. Therefore, whether a reasonable payment fee will be required by third parties or public sector bodies should be clarified.

Finally, we comment on Article 8(6), which states that: *"Unless otherwise provided by Union law, including Article 6 of this Regulation, or national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943"*. Article 8(6) appears to be at odds with Articles 4(3), 5(8) and 19(1) discussed above, given that these provisions specifically envisage the disclosure of trade secrets. The most logical interpretation is that Article 8(6) is stipulating a default rule (i.e. one of non-disclosure of trade secrets in the case of data access (in particular in other Union legislation)) and these specific provisions are exceptions to that rule. However, this provision risks causing confusion and, in any event, such a general provision is not needed because of Article 3(2) of the TSD.[201] At the

[201] Drexl et al (2022), [285].

very least, the role of Article 8(6) needs to be clarified and justified or else it may be better simply to omit it.[202]

5.8 Conclusion

This section has shown that while trade secrets protection may be a flexible tool that can be utilised in the context of the data economy, legal uncertainties exist about how trade secrets protection applies in the data economy. The advantage of waiting for judicial clarification is that this can provide context-specific guidance. However, this may take considerable time. On the other hand, legislative clarification risks intervening too soon, before markets in the data economy have taken shape. Therefore, it is recommended that the EU Commission consider utilising interpretative soft law mechanisms on the applicability of trade secrets protection in the data economy, particularly as regards the criteria for protection as a trade secret. While such soft law would be non-binding, it would indicate the preferred interpretation of trade secrets in the data economy and thus hopefully steer industry behaviour.[203] In addition, the EC might consider issuing guidance through a Frequently Asked Questions (FAQs) section on its website, which it has already done in relation to general features of the TSD.[204]

Second, we suggest that the EU Commission investigate whether existing aspects of the TSD and complementary areas of law – labour law, criminal law and contract law – are undermining the effectiveness of the TSD, such that legislative action needs to be taken. Specifically, the EU Commission should examine further whether:

i) the checks and balances of Articles 3 and 5 of the TSD should apply to factually secret data that does not reach the threshold definition of trade secret (see section 5.4);

ii) the drafting of Article 4(5) of the TSD on infringing goods is leading to excessive protection in relation to the data economy (see section 5.6);

iii) the divergences in regulation of employees and ex-employees in Member States is a barrier to innovation or cross-border sharing of data (see section 5.3);

iv) any divergences in contractual override of reverse engineering in Member States is a barrier to innovation in the data economy (see section 5.4); and

v) divergences in criminal penalties in Member States is a barrier to innovation or cross-border sharing of data (see section 5.6).

These investigations will require ongoing monitoring about the impacts of the TSD and those areas of trade secret law that are unharmonised in the EU.

Third, our recommendation is that the EC should not consider introducing a right for "shared data with limited access" that currently exists in Japan because it is context specific and its positive impact on data sharing is as yet unproven. However, the EU Commission should monitor with interest the impact of the Japanese scheme.

Finally, we think there are aspects of the Data Act Proposal, in relation to trade secrets, which could be further debated. These include: i) whether there should be clarification in either soft law or the recitals to the Data Act that trade secrets protection does not apply

[202] Drexl et al (2022), [284] recommend deleting the provision.

[203] It is appreciated that there is much contention over the influence and impact of EU soft law, which has been investigated at length, for example, in Eliantonio, M., Korkea-aho, E. & Stefan, O. (eds), *EU Soft Law in Member States: Theoretical Findings and Empirical Evidence* (Hart, 2020). See also Andone, C. & Coman-Kund, F., 'Persuasive rather than "binding" EU soft law? An argumentative perspective on the European Commission's soft law instruments in times of crisis' (2022) 10 The Theory and Practice of Legislation 22.

[204] See https://ec.europa.eu/growth/industry/strategy/intellectual-property/trade-secrets/faq-protection-against-unlawful-acquisition-undisclosed-know-how-and-business-information-trade_en.

to raw, machine-generated data, whether individual or in aggregated from; ii) whether the scope of “data” for the purposes of data access obligations should be amended to go beyond raw data to include inferred and derived data; iii) whether guidance should be provided on how and who is to assess “strictly necessary” and “necessary” and “appropriate” measures to protect confidentiality, since if this is left to the parties, it may invariably lead to “overclaiming”, confusion or burdensome requirements; and iv) to revisit whether Article 8(6) should be retained or omitted.

6 Conclusions and recommendations

6.1 Major conclusions

The first major conclusion to be drawn from this study is certainly that the topic of data sharing and the appropriation and protection of data through trade secrets is going to continue to grow in significance in the future. However, only a small share of companies seems to be currently expert in this domain.

Several factors may explain the situation:

- Particularly modern ways of data sharing – such as the sharing of big data sets, e.g., for training AI models – seem to be still in their infancy with many industries. Data that is shared many times seems to involve smaller datasets or data incorporating know-how, shared using bilateral contractual agreements, i.e., practices that have been common for longer periods of time.
- The TSD is a rather new Directive. Firms are still in the process of adapting to the provisions of the Directive and they also need time to define the nexus of the TSD with (novel) ways of sharing data.
- In many firms, there seems to be a lack of clear institutional ownership for trade secrets – particularly in connection with data sharing. Different parts of trade secrets are being dealt with by any combination of legal, IP, IT and corporate security departments. Consequently, specific policies governing the use of trade secrets in firms (generally, and even more so in relation to shared confidential and commercially valuable data) seem to have only recently been developed by firms.

Firms have, therefore, only recently begun to consider the specific roles trade secrets could play in protecting shared confidential and commercially valuable data. In re-organising and adapting their IP policies to the provisions of the TSD, the major use of trade secrets seems to be that of a second layer of protection if/after protection through contracts – which is clearly the most preferred way to regulate data sharing – fails. Trade secrets protection is hence an additional remedy/recourse. It is also a means deemed useful against misappropriation through third parties, with whom no contractual relationships exist. To a certain degree, trade secrets law may also help in the drafting of contracts through the ability to refer to common terminology and concepts.

The usefulness of "trade secrets protection" is hereby often only assumed. In the empirics, there was considerable debate and uncertainty as to the precise meaning of the defining elements of a trade secret, namely about when shared data can be considered commercially valuable to obtain trade secret protection; what is meant by "reasonable steps"; and when data (that is shared, perhaps with many parties) can be considered secret. This was often related to the lack of a developed jurisprudence in Europe – a factor that was also discussed in terms of uncertainty regarding the potential practically to enforce trade secrets.

The legal analysis revealed that some of the uncertainty may not be warranted, if one would refer to jurisprudence, e.g., in the U.S., where very similar legislation is in place. There are, however, some aspects of the TSD, and the relationship of the Directive to other pieces of legislation (employment law, competition law, criminal sanctions) that merit further discussion, without which the use of trade secrets for facilitating data sharing may be hampered.

Overall, the evidence as to whether trade secrets protection facilitates the sharing of data or not remains mixed. While there are instances where trade secrets protection has reported to provide this facilitating role, there have been others where it seems that it can be used to block the sharing of data. A common situation seems to be that many firms in principle recognise and would be willing to share data, but at the same time are reluctant to do so given a) the uncertainties as described above amidst b) a fear that the party who shares the data partly loses the control over the data and/or c) that there is no adequate sharing of benefits and profits, once the party with which the data is shared find a new way to appropriate the data.

6.2 Recommendations

There are three sets of recommendations which we have developed:

- Recommendations aimed at operationally improving firm performance when protecting confidential and commercially valuable data with trade secrets protection
- Recommendations aimed at reducing possible ambiguity when interpreting the current Trade Secrets Directive
- Recommendations aimed at improving and monitoring the legal framework surrounding the use of trade secrets protection for protecting confidential and commercially valuable data

In the following, we describe these three sets of recommendations in greater detail.

6.2.1 Operationally improving firm performance when using trade secrets protection for shared confidential and commercially valuable data

Given the noted scarcity of expert know-how when it comes to trade secrets and data sharing within firms, the most obvious recommendation is to invest in awareness-raising and training in this regard. Respective offerings should seek to develop know-how along two dimensions: legal know-how (also including guidance and interpretation around jurisprudence outside the EU, which could possibly be taken up by European courts) and managerial/process know-how (how to organise the management of confidential information and data in firms, how to govern processes of data sharing).

Given the high significance of contracts in this domain, it is also advisable to create, e.g., contract templates for the sharing of confidential and commercially valuable data governed by trade secrets (in the context of Horizon-Europe, for example, as an additional template along existing contract templates such as DESCA). Company case studies and testimonials may help convey the practicability and importance of the measures to the target audience.

Important multipliers in this regard are, for example, the European IPR Helpdesk (and the international SME helpdesks); the EUIPO (and its awareness-raising and IP observatory activities); national initiatives that foster technology transfer by using IP (like Knowledge Transfer Ireland; or in Austria the National Contact Point IP). The importance of trade secret protection, particularly in the context of data sharing, can also be highlighted in upcoming EU recommendations, such as the revised/amended Codes of Practice for knowledge transfer and valorisation of the EU. Specifically in the context of shared data, bridges and contacts must be sought between the IP community and the mostly technical data sharing community.

6.2.2 Reducing possible ambiguity and improving clearness when interpreting the TSD

For reducing possible ambiguities and improving the understanding of some of the key features of trade secrets protection – beyond what can be conveyed through awareness raising and training – there are two sets of measures which can be considered: the use of explanatory guidelines as well as direct changes in the TSD itself.

Japan has – of course against a different legal tradition – championed the use of guidelines for trade secrets, and additional guidance can be also found in the U.S. UTSA. While these guidelines cannot be replicated 1:1 in Europe, it seems nonetheless worth considering generating a European version of such guidelines (or a respective recommendation) to improve the understanding of the TSD – in the sense of being inspired by the U.S./Japanese examples. Absent developing jurisprudence, it could, for example, be inspired by analogies with the jurisprudence in the U.S. or in Japan, where feasible – for example, when it comes to questions of clarifying the notions of "commercial value" or "reasonable steps".

6.2.3 Improving and monitoring the legal framework surrounding the use of trade secrets for protecting confidential and commercially valuable data

The study has revealed that successful use of trade secrets law for protecting and appropriating confidential and commercially valuable data relies also on a good interaction of the application of trade secret law with other pieces of law. This relates primarily to three bodies of law:

- *Employment law*: Different Member States may have different regulations regarding post-termination clauses. Cases in point are for example periods of times defined by law which can be applied by employers to restrict the ability of former employees to obtain a new job with a competitor for a certain period – one of the reasons being that the competitors do not get a head start with a new employee who can apply prior know-how (and possibly also use confidential and commercially valuable data) from the former employer in the context of the new job. Such regulations can help strengthen trade secret protection particularly in cases where the value of trade secrets diminishes (fast) with time. It would be interesting to monitor whether different national laws on employment mobility influence the use of trade secrets for confidential and commercially valuable data.
- *Criminal law / sanctions*: Most Member States have (different) criminal sanctions in place for misappropriating IP and/or trade secrets. The Japanese example has shown that a) uncertainty regarding whether certain confidential information constitutes a trade secret or not in conjunction with b) the possibility to fall victim to criminal sanctions may impede the use of trade secrets and/or even data sharing, as a means for employees to stay "on the safe side". Again, it would be interesting to monitor whether such interaction and interdependency between criminal sanctions and the use of trade secrets (more specifically, the sharing of confidential and commercially valuable data protected as trades secrets) can be observed.
- *Competition law*: One – as of now – rather theoretical issue could be if a situation ensures where a certain set of data becomes so valuable in a market that having access to this data becomes a matter of necessity. Hence, the role of a possible "dominant" market player exerting full control over such relevant data and its downstream uses should be dealt with specifically. This situation raises questions of abuse of dominant position and bears some similarity to the situation with standard-essential patents (SEPs), where there is then the obligation to license such patents under FRAND terms. The Data Act Proposal is meant to be a solution to this issue in respect – at least - of machine generated data of interconnected devices that affect aftermarket services for those devices. However, its interface with trade secrets protection needs further consideration.

The situations described above do not necessitate a change to the TSD per se and given that evidence of use of trade secrets and the respective jurisprudence is developing, the issue is more of being aware of the possible problems and monitoring whether they materialise in practice. Post-employment restrictions and criminal sanctions regimes may raise the question of whether harmonisation at EU level is needed. This monitoring function – through, e.g., studies, the implementation of working groups – could be made a task for bodies like the EU´s SCDS.

The Japanese model of unfair competition protection for shared data with limited access should be viewed with curiosity but also caution - it seems to have emerged due to a particular understanding of 'trade secret' under Japanese law, without any empirical evidence that trade secret or contractual protection was insufficient and has not yet produced any jurisprudence or been evaluated.

References

Abadi, D., 'Machine vs. human generated data', 30 December 2010 available at http://dbmsmusings.blogspot.com/2010/12/machine-vs-human-generated-data.html.

Almeling, D.S., Snyder, D.W. & Sapoznikow, M., 'A statistical analysis of trade secret litigation in federal courts' (2009) 45 Gonz. L. Rev. 291.

Amir, E., Levi, S. & Livne, T., 'Do firms underreport information on cyber-attacks? Evidence from capital markets' (2018) 23(3) Review of Accounting Studies 1177–1206, available at https://doi.org/10.1007/s11142-018-9452-4.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J.G., Levi, M., Moore, T. & Savage, S., 'Measuring the cost of cybercrime' in Brecht, M. & Nowey, T. (eds) *The economics of information security and privacy* (Springer, 2013), ch 12, pp. 265–300.

Andone, C. & Coman-Kund, F., 'Persuasive rather than "binding" EU soft law? An argumentative perspective on the European Commission's soft law instruments in times of crisis' (2022) 10 The Theory and Practice of Legislation 22.

Andrijcic, E. & Horowitz, B., 'A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property' (2006) 26(4) Risk Analysis 907–923.

Anton, J.J. & Yao, D.A., 'Little patents and big secrets: managing intellectual property' (2004) RAND Journal of Economics 1–22.

Aplin, T., 'Reverse engineering and commercial secrets' (2013) 66 Current Legal Problems 1.

Aplin, T., 'A critical evaluation of the Proposed Trade Secrets Directive' [2014] IPQ 257.

Aplin, T., 'Trading Data in the Digital Economy: Trade Secrets Perspective' in Lohsse, S. Schulze, R. and Staudenmayer, D. (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (2017, Nomos), pp. 59-74.

Aplin, T., 'The limits of trade secret protection in the EU' in Sandeen, S., Rademacher, C. and Ohly, A. (eds) *Research Handbook on Information Law and Governance* (Edward Elgar, 2021) ch 10, pp. 174-194.

Appleyard, M.M., 'How does knowledge flow? Interfirm patterns in the semiconductor industry' (1996) 17 Strategic Management Journal 137–154.

Arora, A., Athreye, S. & Huang, C., 'The paradox of openness revisited: Collaborative innovation and patenting by UK innovators' (2016) 45(7) Research Policy 1352-1361, available at https://doi.org/10.1016/j.respol.2016.03.019.

Arrow, K., 'Economic Welfare and the Allocation of Resources for Invention' in National Bureau of Economic Research, *The Rate and Direction of Inventive Activity: Economic and Social Factors* (1962, Princeton University Press), pp. 609-626.

Arundel, A., 'The relative effectiveness of patents and secrecy for appropriation' (2021) 30(4) Research Policy 611–624, available at https://doi.org/10.1016/S0048-7333(00)00100-1.

Beale, A. & Foulser McFarlane, J., 'The importance of keeping your company's trade secrets, secret' available at https://www.ipcybersecurity.com/free-guide-1.

Bently, L., Bodea, G., Calatrava, M.C., Chicot, J., Derclaye, E., Domini, A., Fisher, R., Gkogka, A., Karanikolova, K., Misojcic, M. & Radauer, A., *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases* (2018).

Borghi, M. & Karapapa, S., 'Contractual restrictions on lawful use of information: sole-source databases protected by the back door?' [2015] EIPR 505.

Campmas, et al. (n.Y.): Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting cooperative, connected and automated mobility. EASME/COSME/2018/004.

CapGemini invent, et al., *B2 – Analytical report on EU law applicable to sharing of non-personal data. Support centre for data sharing* (2020).

Cash, M.H., 'Keep It Secret, Keep It Safe: Protecting Trade Secrets by Revisiting the Reasonable Efforts Requirement in Federal Law' (2015) 23 J. Intell. Prop. L. 263.

Chesbrough, H., 'The Future of Open Innovation' (2017) 60(1) Research-Technology Management, 35–38, available at https://doi.org/10.1080/08956308.2017.1255054.

Chesbrough, H.W., *Open innovation: The new imperative for creating and profiting from technology*. (Harvard Business Press, 2003).

Cohen, W., Nelson, R., & Walsh, J., 'Protecting their Intellectual Assets: Appropriability conditions and why firm patent and why they do not in the American manufacturing sector' (2000) National Bureau of Economic Research Working Paper Series 7552.

Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014 on the Proposal of the European Commission for a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure of 28 November 2013, COM (2013) 813 in (2014) 45 IIC 953.

Crass, D., Garcia Valero, F., Pitton, F., & Rammer, C., 'Protecting Innovation Through Patents and Trade Secrets: Evidence for Firms with a Single Innovation' (2019) 26(1) International Journal of the Economics of Business 117–156, available at https://doi.org/10.1080/13571516.2019.1553291.

Denicolo, V., & Alberto Franzoni, L., 'Patents, Secrets, and the First-Inventor Defense' (2004) 13(3) Journal of Economics Management Strategy 517–538, available at https://doi.org/10.1111/j.1430-9134.2004.00021.x.

Dittmer, S. & Pooley, J. (lead authors). *Protecting Trade Secrets – Recent EU and U.S. reforms* (International Chamber of Commerce, 2019).

de Jongh, T., Radauer, A., Bostyn, S. & Poort, J., *Effects of Supplementary Protection Mechanisms for Pharmaceutical Products*: *Final Report* (2018).

De Vroey, M. & Allaerts, M., 'Trade secrets protection: an interim update of Belgian and EU case law' (2021) 16 JIPLP 1391.

Domeij, B., 'The Trade Secrets Directive and employees' in Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonisation and Protection of Trade Secrets in the EU* (Edward Elgar, 2020), ch 9, pp. 151-172.

Donegan, C. & Vella, M., 'IP monetisation: what might the future hold?' in: iam March/April 2019. Accessed via https://www.iam-media.com/article/ip-monetisation-what-might-the-future-hold.

Drexl, J., 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) JIPITEC 257.

Drexl, J., *Data Access and Control in the Era of Connected Devices, Study on behalf of BEUC* (2018) available at https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf.

Drexl, J. & Hilty, R. et al., 'Technical Aspects of Artificial Intelligence: An Understanding from an Intellectual Property Law Perspective' (October 8, 2019). Max Planck Institute for Innovation & Competition Research Paper No. 19-13, available at SSRN: https://ssrn.com/abstract=3465577.

Drexl, J., Banda, C., González Otero, B., Hoffmann, J., Kim, D., Kulhari, S., Moscon, V., Richter, H. & Widemann, K., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act) (2022), available at https://www.ip.mpg.de/en/research/research-news/position-statement-on-the-eu-data-act.html

Eliantonio, M., Korkea-aho, E. & Stefan, O. (eds), *EU Soft Law in Member States: Theoretical Findings and Empirical Evidence* (Hart, 2020).

EUIPO, *The Baseline of Trade Secrets Litigations in the EU Member States* (2018).

European Commission, 'Staff Working Document on the free flow of data and emerging issues of the European data economy' SWD (2017) 2 final.

European Commission, Directorate-General for Communications Networks, Content and Technology, Scaria, E., Berghmans, A., Pont, M., et al., *Study on data sharing between companies in Europe: final report*, Publications Office, 2018, available at https://data.europa.eu/doi/10.2759/354943.

European Commission, Directorate-General for Competition, Montjoye, Y., Schweitzer, H., Crémer, J., *Competition policy for the digital era*, Publications Office, 2019, available at https://data.europa.eu/doi/10.2763/407537.

European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, *The scale and impact of industrial espionage and theft of trade secrets through cyber*, Publications Office, 2019, available at https://data.europa.eu/doi/10.2873/48055.

European Commission, *A European Strategy for Data,* Brussels 19.2.200, COM (2020) 66 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN.

European Commission, Executive Agency for Small and Medium-sized Enterprises, *Big Data and B2B platforms : the next big opportunity for Europe: final report*, Publications Office, 2021, available at https://data.europa.eu/doi/10.2826/70258.

European Commission, *Public Consultation on the Data Act: Summary Report* (2021), available at https://digital-strategy.ec.europa.eu/en/public-consultation-data-act-summary-report.

Friedman, D.D., Landes, W. M., Posner, R.A., Journal, T., & Winter, N. 'Some economics of trade secret law' (1991) 5(1) Journal of Economic Perspectives 61–72.

Georgescu, A.-A. E. P., & PWC. (2018). Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber. https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf.

Germany (2021) 52(6) IIC 775.

Gordon, L.A., & Loeb, M.P., 'The economics of information security investment' (2002) 5(4) ACM Transactions on Information and System Security (TISSEC) 438–457.

Hall, B., Helmers, C., Rogers, M. & Sena, V. (2012). The use of alternatives to patents and limits to incentives, available at https://www.gov.uk/government/publications/the-use-of-alternatives-to-patents-and-limits-to-incentives.

Hrdy, C.A., 'The Value in Secrecy' (August 2, 2021). Available at https://ssrn.com/abstract=3897949 or http://dx.doi.org/10.2139/ssrn.3897949.

Holgersson, M., 'Patent management in entrepreneurial SMEs: a literature review and an empirical study of innovation appropriation, patent propensity, and motives' (2013) 43(1) R&D Management 21–36, available at https://doi.org/10.1111/j.1467-9310.2012.00700.x

Iacob, N. & Simonelli, F., *Big Data and B2B platforms: the next big opportunity for Europe – Report on market deficiencies and regulatory barriers affecting the creation of EU-wide B2B health data marketplaces and unified diabetes-related datasets*. EASME/COSME/2018/004.

Kerber, W. & Gill, D., 'Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation' (2019) 10 JIPITEC 244.

Kerber, W., 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (April 08, 2022), available at https://ssrn.com/abstract=4080436 or http://dx.doi.org/10.2139/ssrn.4080436.

King, A.W., 'Disentangling interfirm and intrafirm causal ambiguity: A conceptual model of causal ambiguity and sustainable competitive advantage' (2007) 32(1) Academy of Management Review 156–178, available at https://doi.org/10.5465/AMR.2007.23464002.

Kolasa, M., *Trade Secrets and Employee Mobility: In Search of an Equilibrium* (CUP, 2018).

Lagazio, M., Sherif, N., & Cushman, M., 'A multi-level approach to understanding the impact of cyber crime on the financial sector' (2014) 45 Computers & Security 58–74.

Lapousterle, J., Geiger, C., Olszak, N., & Desaunettes, L., 'What protection for trade secrets in the European Union? A comment on the directive proposal' [2016] EIPR 255.

Lee, N., 'Protection for artificial intelligence in personalised medicine – the patent/trade secret tradeoff' in J Schovsbo, J., Minssen, T. and Riis, T. (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar, 2020), ch 14, pp. 269-296.

Leiponen, A. & Byma, J., 'If you cannot block, you better run: Small firms, cooperative innovation, and appropriation strategies' (2009) 38(9) Research Policy 1478–1488, available at https://doi.org/10.1016/j.respol.2009.06.003.

Leistner, M., 'The existing European IP rights system and the data economy – An overview with particular focus on data access and portability' in Josef Drexl et al (eds), *Data Access, Consumer Protection and Public Welfare* (Nomos 2021), pp. 209-251, available at https://doi.org/10.5771/9783748924999.

Levine, D.S. & Sichelman, T., 'Why do startups use trade secrets' (2018) 94 Notre Dame L. Rev. 751.

Martinis, L. de, Gaudino, F. & Respess III, T.S., *Study on Trade Secrets and Confidential Business Information in the Internal Market: Final Study* (April, 2013).

Mayer-Schönberger, V. & Cukier, K., *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray 2013).

Milgrim, R.M. & Bensen, Eric. E., *Milgrim on Trade Secrets* (Lexis Nexis).

Ministry of Economy, Trade and Industry, *Guidelines on Shared Data with Limited Access,* 23 January 2019. available at https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines_on_shared_data_with_limited_access.pdf.

Ministry of Economy, Trade and Industry, *Management Guidelines for Trade Secrets*, available at https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/0813mgtc.pdf.

Mylly, U., 'Freedom of the media and trade secrets in Europe' in Sandeen, S., Rademacher, C. & Ohly, A. (eds) *Research Handbook on Information Law and Governance* (Edward Elgar*,* 2021) ch 11, pp. 195-216.

Nordberg, A., 'Trade secrets, big data and artificial intelligence' in Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar, 2020), ch 11, pp. 194-220.

Noto La Diega, G. & Sappa, C., 'The Internet of Things at the intersection of data protection and trade secrets. Non-conventional paths to counter data appropriation and empower consumers' (2020) 3 European Journal of Consumer Law 419, available at https://ssrn.com/abstract=3772700.

OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, 26 November 2019.

Ohly, A., 'Germany: The Trade Secrets Protection Act of 2019' in Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonisation and Protection of Trade Secrets in the EU* (Edward Elgar, 2020), ch 7, pp. 104-124.

Ottoz, E. & Cugno, F., 'Patent-Secret Mix in Complex Product Firms' (2008) 10(1) American Law and Economics Review 142-158.

Panagopoulos, A. & Park, I., 'Patents As Negotiating Assets: Patenting Versus Secrecy For Startups' (2018) 128 The Economic Journal 2876–2894, available at https://doi.org/10.1111/ecoj.12540.

Peng, K., Mathur, A. & Narayanan, A., 'Mitigating dataset harms requires stewardship: Lessons from 1000 papers' Draft paper 9 August 2021, available at https://openreview.net/forum?id=KGeAHDH4njY.

Poland (2020) 51(9) IIC 1129.

Pooley, J.A., *Trade Secrets* (Law Journal Press).

Reid, G.C., Searle, N. & Vishnubhakat, S., 'What's It Worth to Keep a Secret' (2014) 13 Duke L. & Tech. Rev. 116.

Ritala, P., Olander, H., Michailova, S. & Husted, K., 'Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study' (2015) 35 Technovation 22–31, available at https://doi.org/10.1016/j.technovation.2014.07.011.

Rowe, E.A. & Sandeen, S.K., *Trade Secrets Law: Cases and Materials* 3rd ed (West Academic).

Sandeen, S.K., ‘The limits of trade secret law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on which it is based’ in Dreyfuss, R. C. and Strandburg, K. J. (eds) *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (Edward Elgar 2011), ch 20.

Sandeen, S.K., ‘Implementing the EU Trade Secrets Directive: a view from the United States’ [2017] EIPR 4.

Sandeen, S.K. & Rowe, E.A., *Trade Secret Law* 2nd edition (West Academic Publishing, 2018).

Sandeen, S.K. & Mylly, U., ‘Trade secrets and the right to information: A comparative analysis of EU and US approaches to freedom of expression and whistleblowing’ (2020) 21 North Carolina Journal of Law and Technology 1, available at: https://scholarship.law.unc.edu/ncjolt/vol21/iss3/2.

Sandeen, S.K. & Aplin, T., 'Trade Secrecy, Factual Secrecy and the Hype Surrounding AI' in Abbott, R. (ed) *Research Handbook on Intellectual Property and Artificial Intelligence* (Edward Elgar, 2022), ch 24, pp. 442-459, available at SSRN: https://ssrn.com/abstract=3929928.

Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonisation and Protection of Trade Secrets in the EU* (Edward Elgar, 2020).

Schovsbo, J., ‘The Directive on trade secrets and its background’ in Schovsbo, J., Minssen, T. & Riis, T. (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar, 2020), ch 2, pp. 7-21.

Senden, L., *Soft Law in European Community Law* (Hart, 2004).

Shinall*,* V., ‘The 5 Types of Sensor Data Used by Businesses & Organisations’ (2019) available at https://blog.temboo.com/5-types-of-sensor-data/.

Sousa e Silva, N., ‘What exactly is a trade secret under the proposed directive?’ (2014) 9 JIPLP 923.

Suzuki, M., ‘Japan’ in Kung-Chung Liu & Reto Hilty (eds), *Trade Secret Protection: Asia at the Crossroads* (Kluwer, 2021), ch 1.

Thomä, J. & Bizer, K., ‘To protect or not to protect? Modes of appropriability in the small enterprise sector’ (2013) 42 Research Policy 35-49.

The Economist., ‘Fuel of the future – Data is giving rise to a new economy’, Briefing 6 May 2017 edition.

Van Caenegem, W., *Trade Secrets and Intellectual Property: Breach of Confidence, Misappropriation and Unfair Competition* (Wolters Kluwer, 2014).

Wajsman, N., & García-Valero, F. (2017). *Protecting Innovation through Trade Secrets and Patents: Determinants for European Union Firms*. European Union Intellectual Property Office. European Observatory on Infringements of Intellectual Property Rights.

Wang, R., ‘Information asymmetry and the inefficiency of informal IP strategies within employment relationships’ (2021) 162 Technological Forecasting and Social Change 120335, available at https://doi.org/10.1016/j.techfore.2020.120335.

Wei, H., Frincke, D., Alves-Foss, J., Soule, T., & Pforsich, H., ’A layered decision model for cost-effective network defense’ (2005) Information Reuse and Integration, Conf, . IRI-2005 IEEE International Conference On., 506–511.

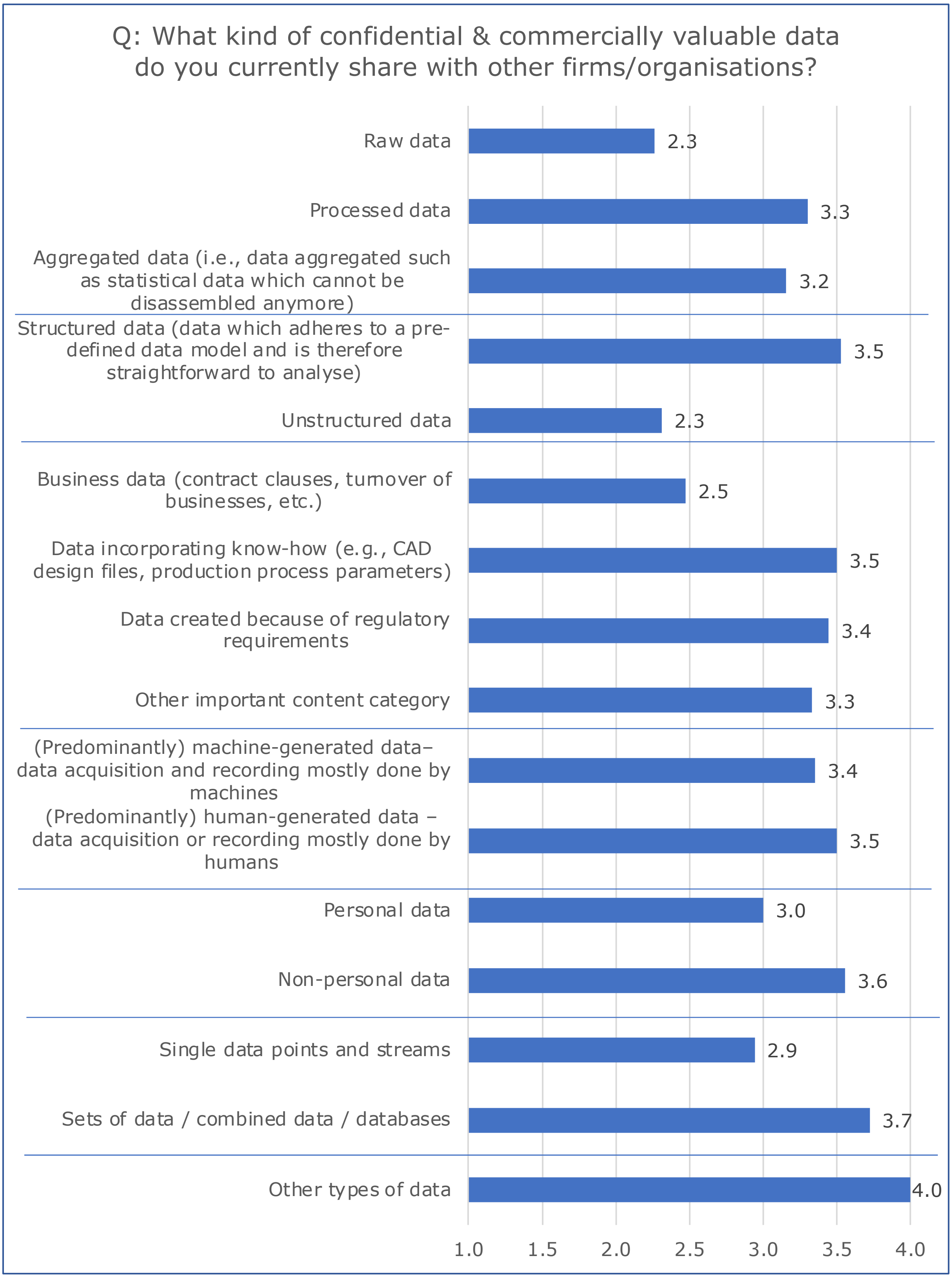
Wennakoski, A. A., ‘Trade secrets under review: a comparative analysis of the protection of trade secrets in the EU and in the US’ [2016] EIPR 154.

World Economic Forum (2011). *Personal Data: The Emergence of a New Asset Class*. https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

XMPro, ‘7 Types of Industrial IoT Data Sources (And How To Use Them)’, available at https://xmpro.com/7-types-industrial-iot-data-sources/ (last accessed September 2022).

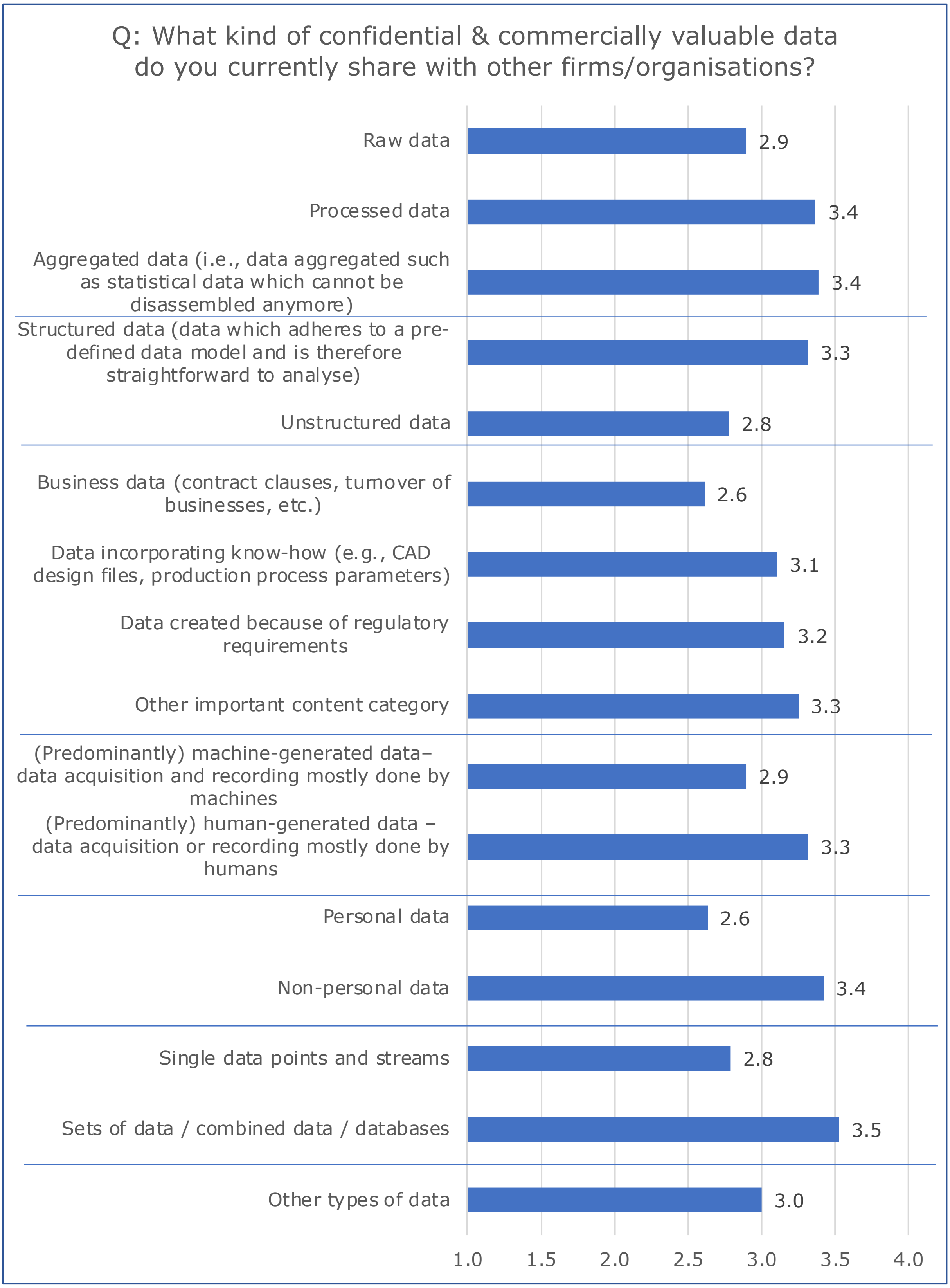
Annex A – Sectorial breakdowns of survey data for the relevance of different types of shared confidential and commercially valuable data

Figure 26 Relevance of different types of shared confidential and commercially valuable data, sector: automotive *)



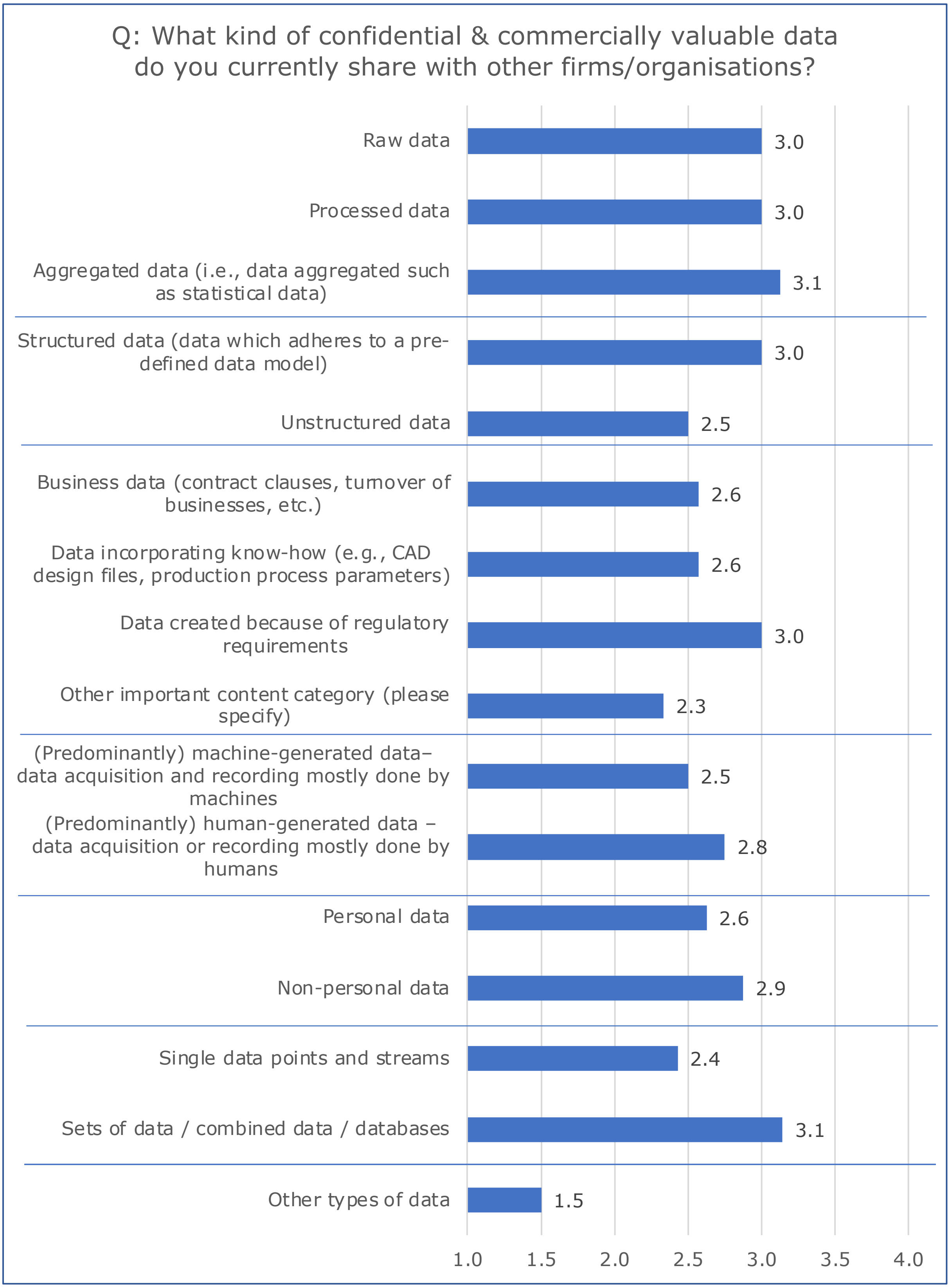
*) arithmetic means of answers on a scale from 1=irrelevant to 4= relevant
Source: Survey, n=16-20

Figure 27 Relevance of different types of shared confidential and commercially valuable data, sector: Health/LS *)



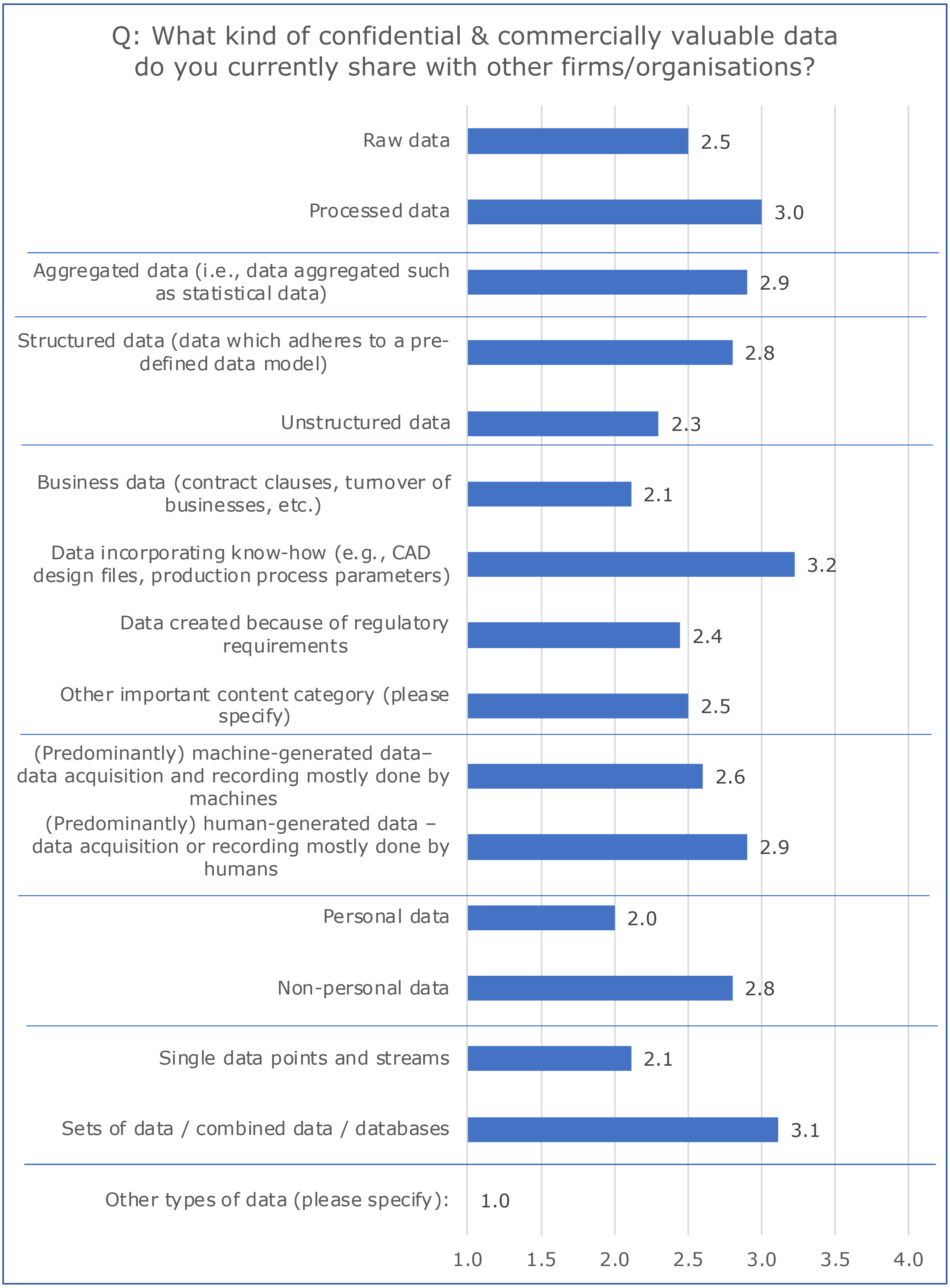
*) arithmetic means of answers on a scale from 1=irrelevant to 4= relevant
Source: Survey, n=18-19

Figure 28 Relevance of different types of shared confidential and commercially valuable data, sector: Financial services *)



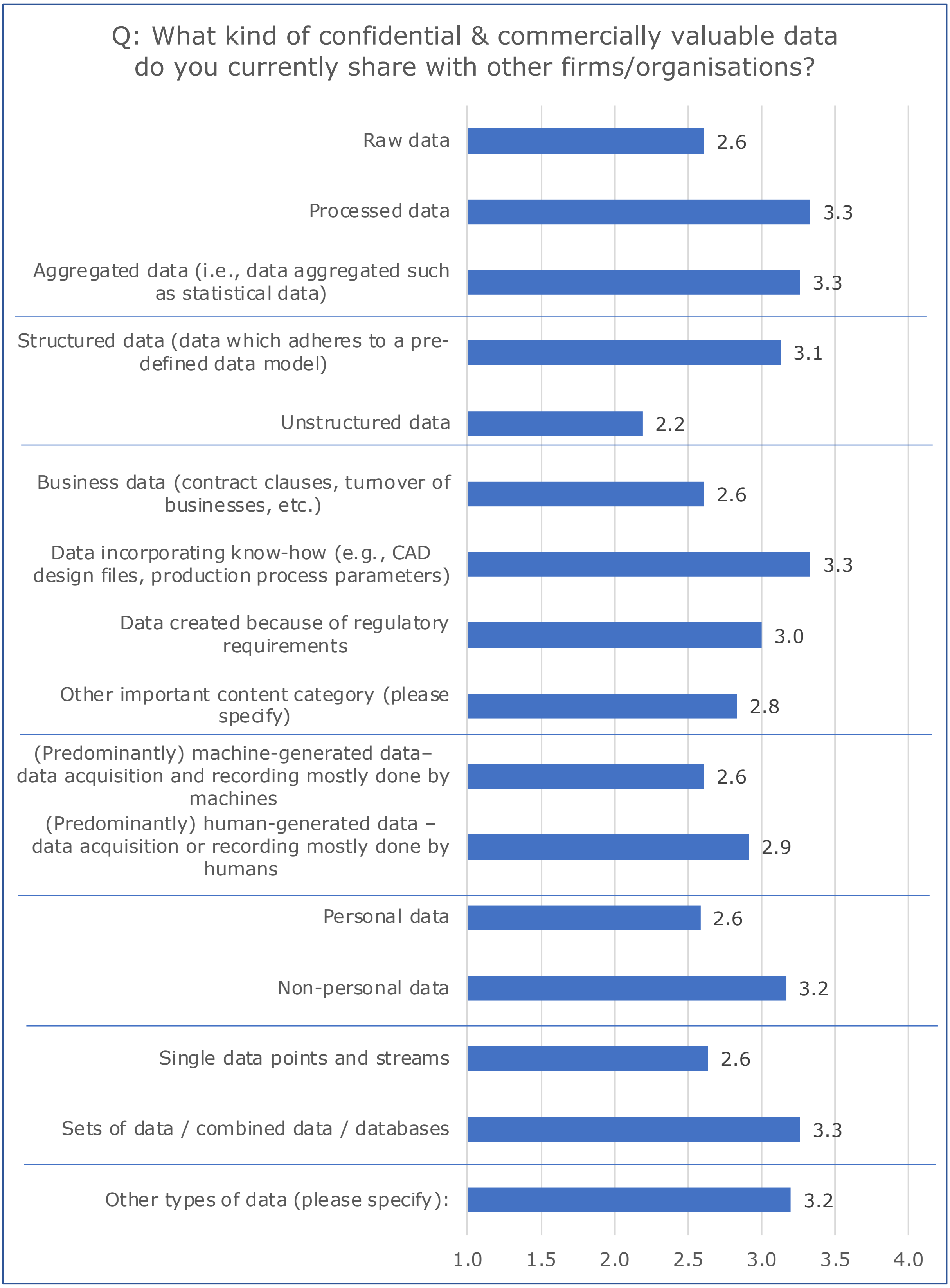
*) arithmetic means of answers on a scale from 1=irrelevant to 4= relevant
Source: Survey, n=6-8

Figure 29 Relevance of different types of shared confidential and commercially valuable data, sector: Energy *)



*) arithmetic means of answers on a scale from 1=irrelevant to 4= relevant
Source: Survey, n=9-10

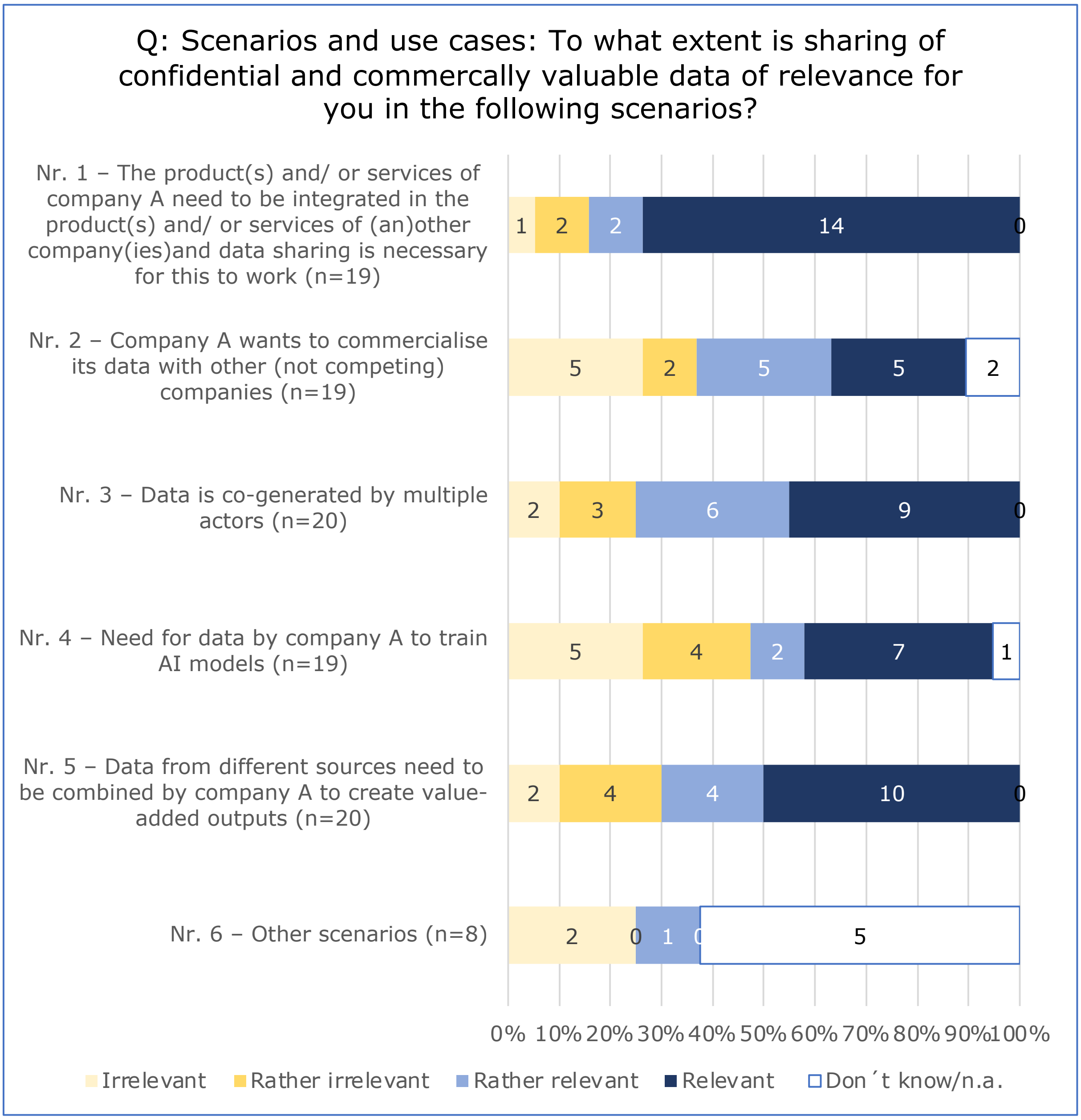
Figure 30 Relevance of different types of shared confidential and commercially valuable data, other sectors *)



*) arithmetic means of answers on a scale from 1=irrelevant to 4= relevant
Source: Survey, n=22-24

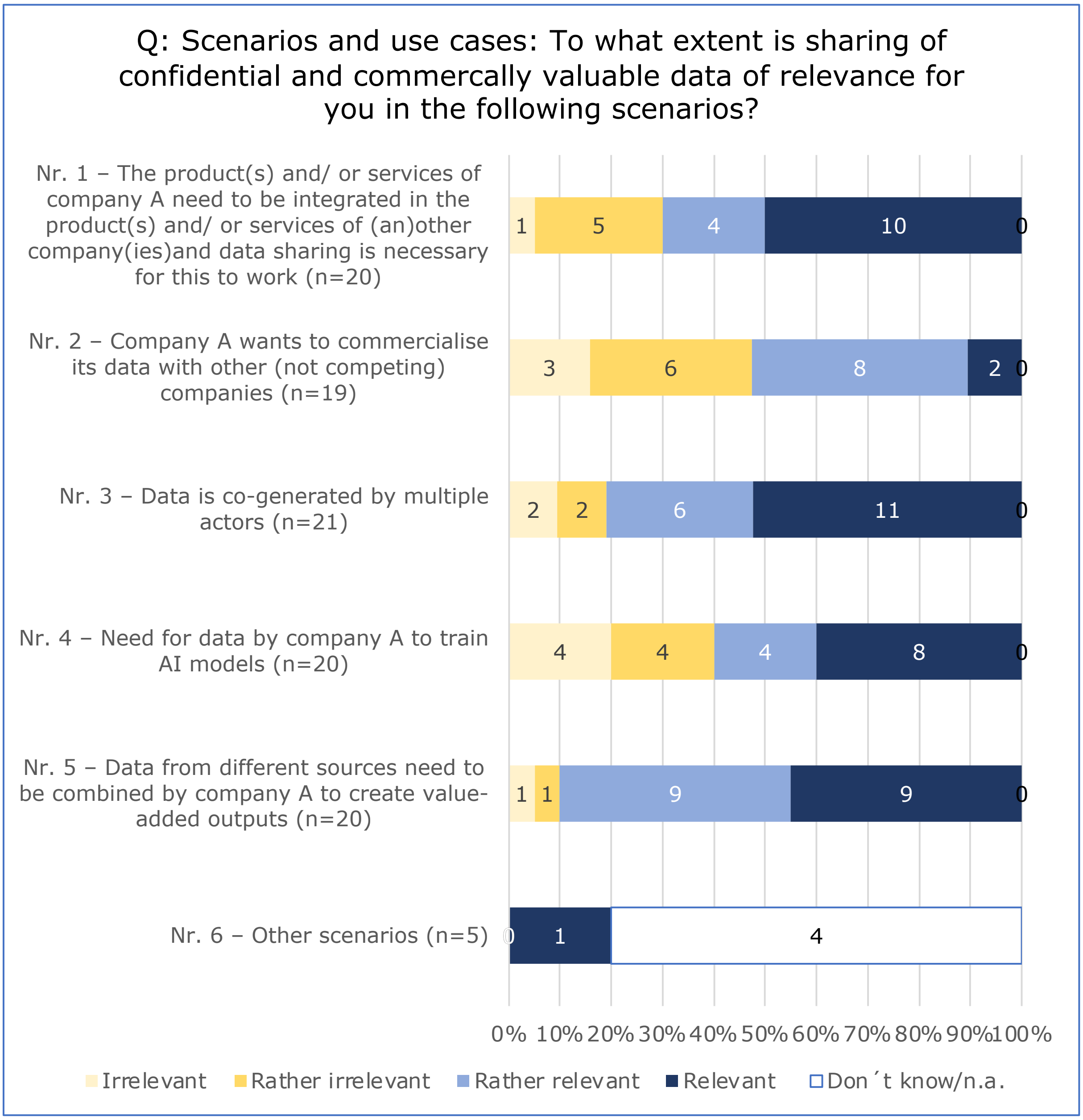
Annex B – Scenarios of data sharing in the survey by sectors

Figure 31 Relevance of different scenarios of data sharing, respondents in absolute numbers, sector: automotive



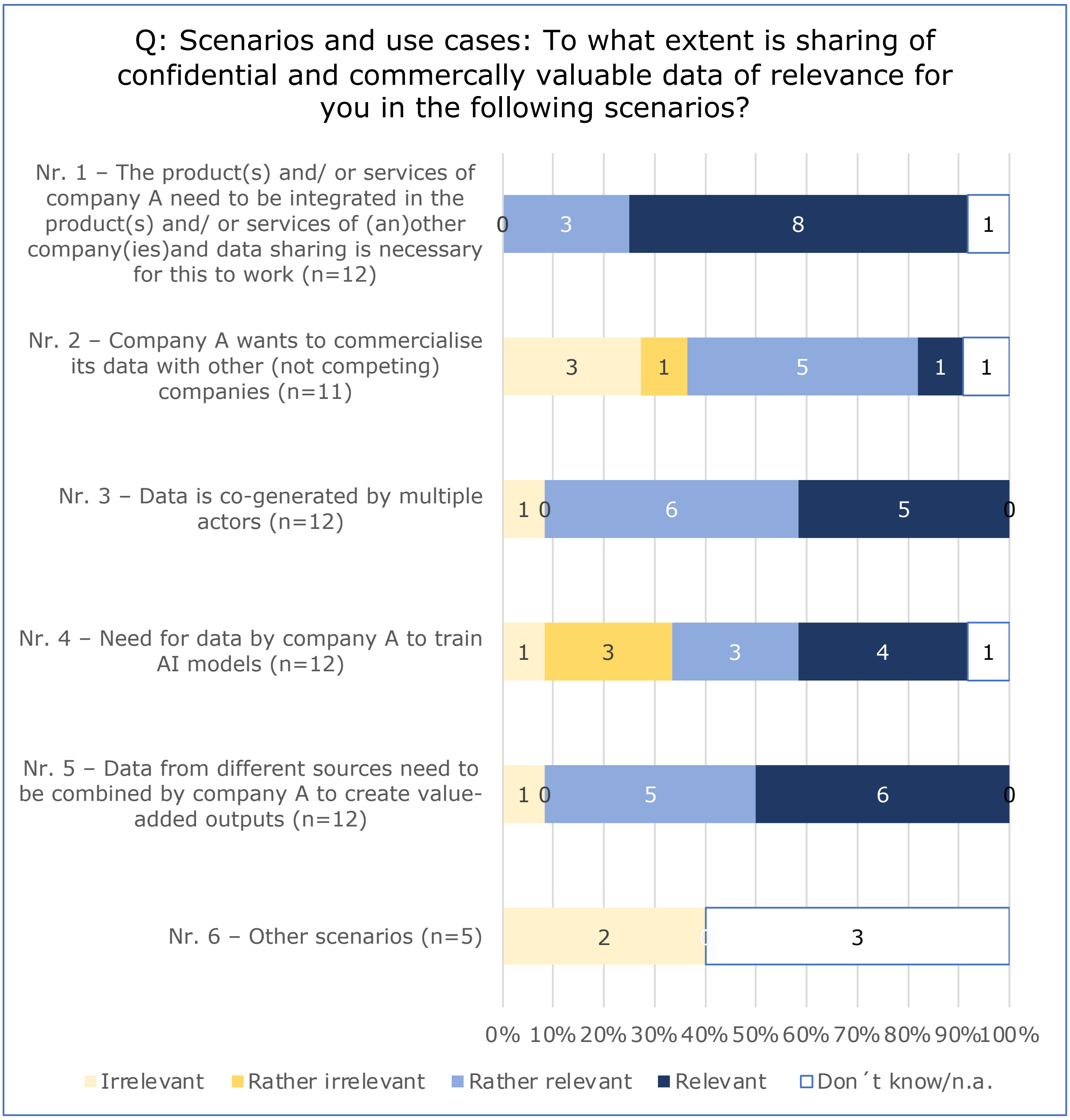
Source: Survey

Figure 32 Relevance of different scenarios of data sharing, respondents in absolute numbers, sector: health/LS



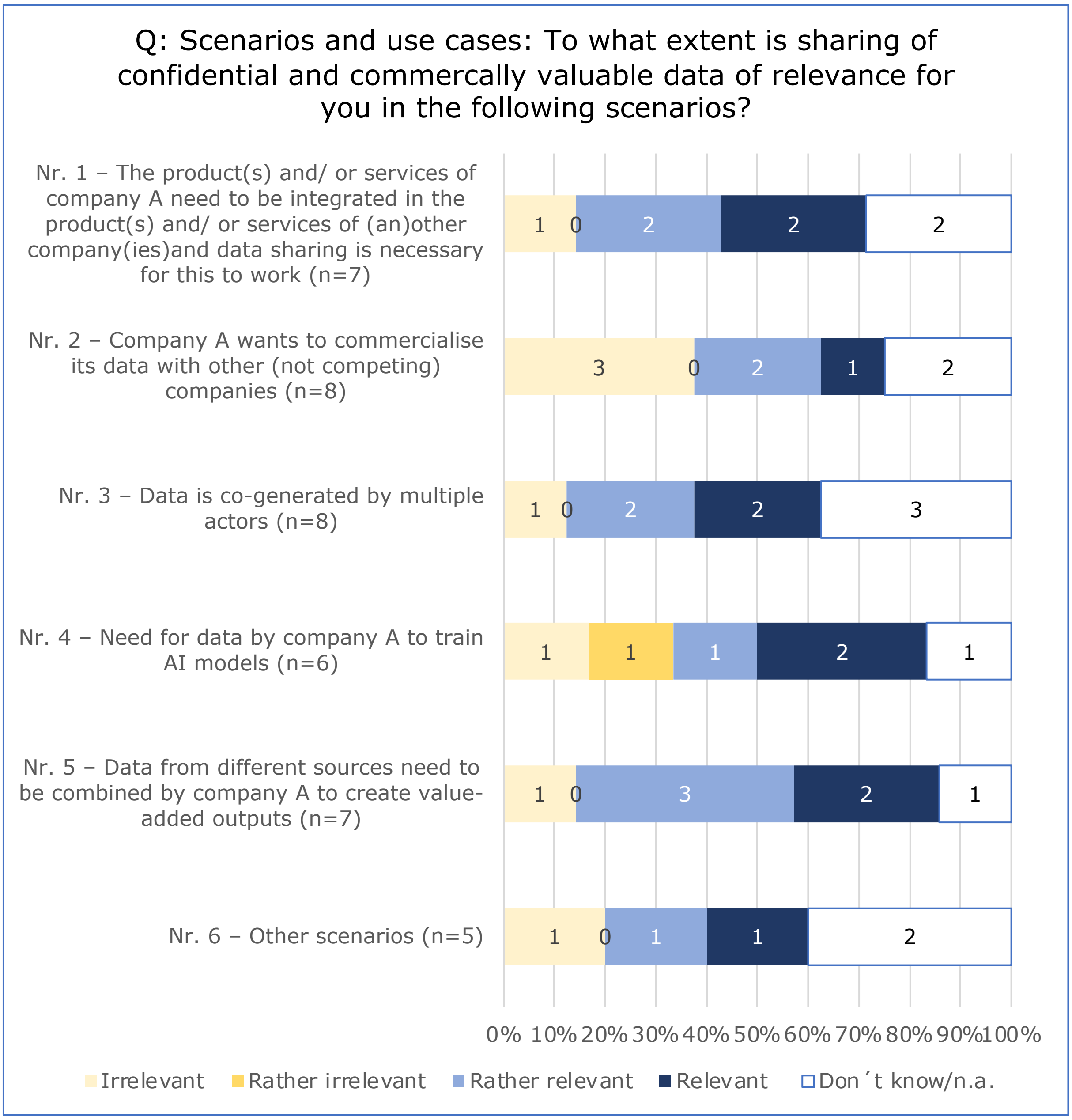
Source: Survey

Figure 33 Relevance of different scenarios of data sharing, respondents in absolute numbers, sector: energy



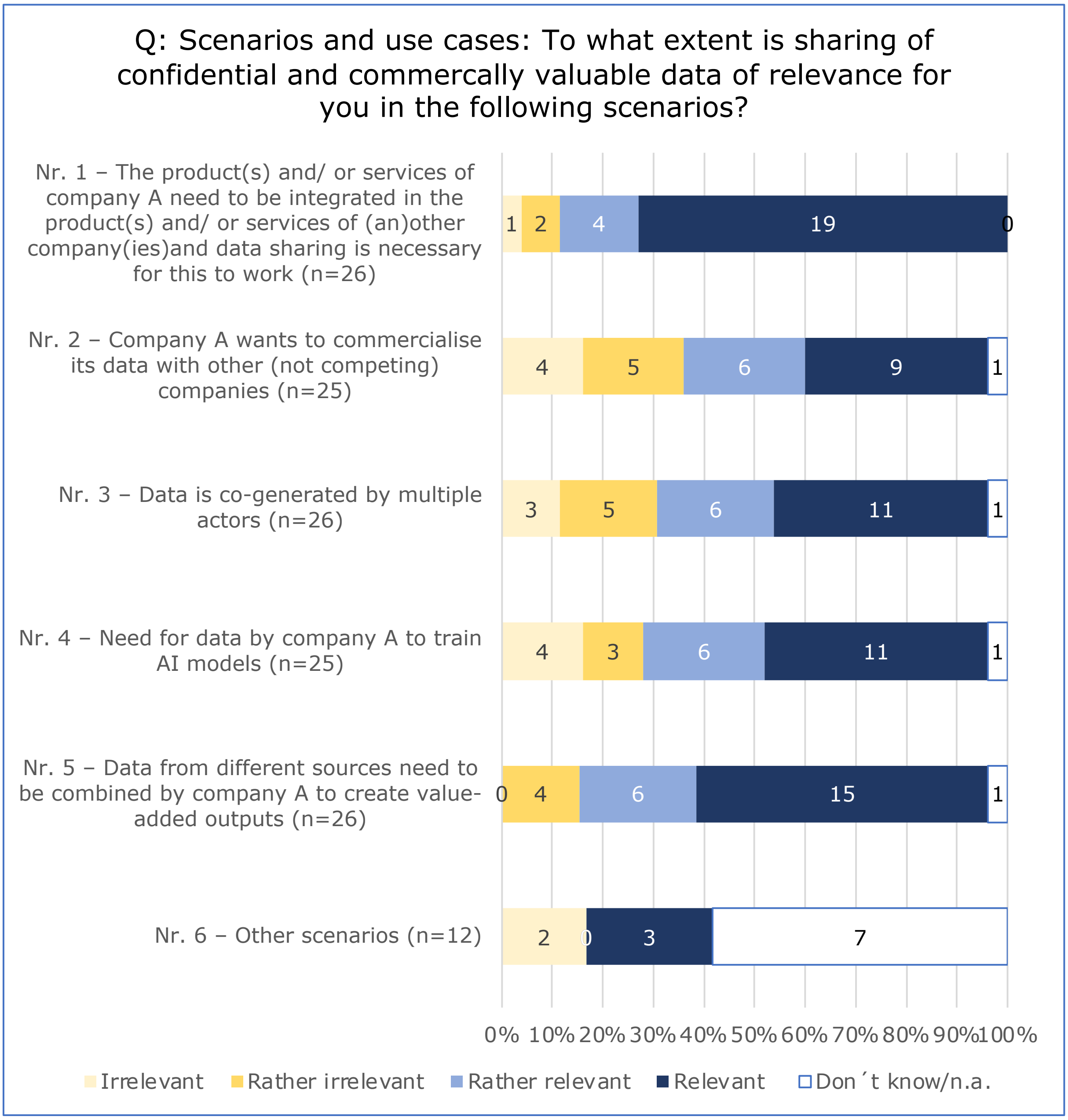
Source: Survey

Figure 34 Relevance of different scenarios of data sharing, respondents in absolute numbers, sector: financial services



Source: Survey

Figure 35 Relevance of different scenarios of data sharing, respondents in absolute numbers, sector: other



Source: Survey

Appendix C – Case studies

Case study Nr. 1: Energy utility firm and its beginning journey into confidential and commercially valuable data sharing and trade secret usage

Sector:	Utilities (energy)
Type of organisation:	Large firm
Type of data shared:	Various
Data shared with:	Service providers, collaboration partners
Use of trade secrets:	Yes

The company in this case study is a leading energy utilities firm in a small EU Member State, selling electrical energy, natural gas, and district heating. Its activities include electricity and heat generation, distribution of electricity, natural gas and heat and cooling, energy consulting and energy services, heat grid provision and expansion, waste utilization, property management, telecommunications and electromobility. The interview was conducted as group interview with three employees. Interviewee 1 is the company's Chief Information Security Officer (CISO) with a degree in data technology and has been with the company for 10 years. Interviewee 2 is a lawyer entrusted with the legal issues surrounding data protection law and compliance. Interviewee 3 is the company's data protection officer with a degree in law and has been with the company since 2015.

While the company attaches great importance to the current sharing of data, the importance is even greater in the foreseeable future due to increasing digital transformation and technical facilitation. They acknowledge that the requirements from the business sector for the shared use of data are increasing as are the platforms and projects that have precisely this goal. Projects themselves are largely in the pilot phase to gain experience with this topic. A special focus is being put on data governance to be able to deal with clear specifications and terms. In the past, the company has gained experience, especially within the framework of cooperation agreements, consulting contracts as well as services/ contract processing for operative business areas and IT, purchasing, services, sales, and distribution.

Data is shared with companies within the group, service providers (within and outside the group) as well as collaboration partners. Data is shared first and foremost to handle business operations professionally, appropriately, and efficiently. The scenarios of data sharing take place in all business areas at almost all levels, depending on the needs of business operations within the framework of specialisations based on the division of labour, within the framework of cooperation agreements or service agreements, considering appropriate competition, strategy, and confidentiality considerations. Other reasons include contract fulfilment, product development and location assessments. Against this backdrop data that could potentially be shared include machine data (e.g., sensor-generated energy data, metering data), data from cloud storage, personal data (e. consumption behaviour, billing data), industry specific data (e.g., effects of technology in terms of temperature, efficiency), marketing data (often public data, such as prices, anyway, but also forecasts), asset data. Barriers for not sharing data include concerns that the competition could gain a competitive advantage through knowledge of one's own trade secrets. These barriers can also be differentiated according to the degree of secrecy: reasons of competition, strategy, no sufficient level of data protection in technical or legal terms.

The prevailing view is that the protection of shared data can only function organisationally by means of a set of rules from a legal and organisational perspective, which is then implemented technically. Protection of shared data is established through measures agreed in procurement/cooperation/service/consultancy/processor contracts. However, as a competitive business, the energy provider is generally restrictive in sharing confidential and commercially valuable. This results on the one hand from legal restrictions but also from (feared) competitive disadvantages. The extent to which competitive advantages could also arise from this is still barely known or researched. The energy producer has addressed the issue of data sharing using declaration or agreement of TOMs (technical-organisational measures), contractual obligations to maintain secrecy, e.g., with penalties, declarations of confidentiality as well as controlled data sharing via established API platform with corresponding access requirements (e.g., contracts) and IT-technical measures. From a data protection perspective, the focus is on personal data of natural persons. The importance of confidentiality, however, encompasses all data, not only personal data, so that collaboration is made possible. While all data should be deleted or access to it should be blocked after termination of the agreements, there is a major problem in obtaining knowledge and evidence of violations of agreements to protect shared confidential and commercially valuable data.

The company uses the instrument of trade secrets from the perspective of information security. The EU Directive 2016/943 was implemented by reviewing and revising/adding to contracts and clauses (sales, purchasing, personnel), NDAs, confidentiality notices, corporate guidelines. Further discussion of this matter takes place together with the data protection and legal departments, if necessary.

In summary, it can be stated that the handling of confidential and commercially valuable data will certainly gain in importance in the near future, as additional insights can often be gained by aggregating a wide variety of data. It is important to have internal rules so that everyone involved is aware of how to deal with such data and the special sensitivity of this topic. With the inevitably extensive (and in the future foreseeably even greater) use of large IT service providers and cloud providers, it is not always possible to check whether they are not using the data for their own or other purposes or disclosing it to authorities for whatever reason; under this aspect, the protection of confidential and commercially valuable data is only a relative one. This is not assessable regarding the protection of patents, copyright, database rights and other IP rights for the companies concerned, nor can it be shaped by contracts (even for large companies). Due to increasing digitalisation and the further development of technical possibilities, this topic will gain in importance, and it will therefore become increasingly important to create the appropriate legal and technical framework conditions.

Case Study Nr. 2: A health business company where data is currently mostly shared in the scope of R&D projects

Sector:	Health
Type of organisation:	Large firm
Type of data shared:	R&D data
Data shared with:	research partners, universities, research organisations, customers and funding agencies
Use of trade secrets:	Yes (but rarely)

The company for this case study is part of the health business, with headquarters in Switzerland. The interviewed partner has a background as PhD Engineer and is heading the firm´s life science technology department.

The firm is generally sharing some confidential and commercially valuable data within EU-projects. Important to remark is that open access is pushed. This means exchanging mostly data which is not seen to be confidential by the firm. Within collaborative research projects confidential and commercially valuable data as well as public data is shared, i.e., data which is not confidential for the firm.

Confidential and commercially valuable data and public data will be shared with and received from research partners, universities, research organisations, customers, and funding agencies. No data sharing with direct competitors takes place. Officially the confidential and commercially valuable data exchange will only happen when an NDA or a contract with a confidentiality clause is in place. However, unofficially, some projects are only based on trust which the firm sees also as a viable way to proceed under certain circumstances. By default, all internally produced data are regarded as confidential by the firm. The company has an approval process for all scientific and personal data in place.

Typical motives for sharing confidential and commercially valuable data are for combining data to achieve common goals with the business partners. The reasons not to share confidential and commercially valuable data are no trust in the partners, no legal agreement in place with the business partner as well as fear of losing value. In today's business the company is sharing confidential and commercially valuable data on a confidential (NDA) and/or on a trust basis. The company states that in the future confidential and commercially valuable data sharing will become key for innovation for them. To manage confidentiality, the firm classifies technical data with restricted access into specific folders, a process that is also undertaken with contractual data for employees and with data where partner provide and/or have access to. In the future, training of global leaders is planned for the classification of managerial data.

The application of trade secrets for protecting confidential and commercially valuable data is seen as *"good behaviour"*. (interview) Trade secrets are, however, applied currently rather rarely when sharing. The mission in tech transfer is to *"pass on data with no trade secret declaration".* (interview) This implies passing on mostly data which is public and not confidential. The employees and business partners in turn do not need to keep data confidential, and the data sharing will be easy among all project partners. The firm is using patent protection as early as possible and hereby "protects" also some of its valuable data and assets which is seen as best way to protect innovation and to earn money.

The major take-away from this case is when a firm is using the contractual protection with declared confidentiality clauses combined with formal IP protection, trade secrets may not be as important for the business for data sharing.

Case Study Nr. 3: OEM automotive supplier illustrating the many different types of confidential and commercially valuable data shared and arguing

Sector:	Automotive supplier
Type of organisation:	Large firm
Type of data shared:	Contracts, production-related data, training data sets for AI
Data shared with:	Research partners, universities, research organisations, customers and funding agencies
Use of trade secrets:	Yes (but rarely)

Generally, the motives for automotive suppliers (like the one in this case study) to share confidential and commercially valuable data is by demand of OEMs, e.g., for quality management and legal/liability purposes as well as for potential future business models based on data.

For automotive suppliers there are in general the following typical cases for sharing confidential and commercially valuable data:

- M&A-activities (buying/selling) and the related necessary exchange of data (contracts, often according to U.S. or UK law).
- By demand of OEMs (contractual topic). There is demand for the exchange of data on production, per single product (e.g., technical data/parameters such as on pressure, temperature, etc.), e.g., for liability purposes. The supplier is, however, hesitant to provide this kind of data as this is considered core know that is not supposed to be shared. Such data should be only internally used, e.g., for quality management, predictive management.
- Training data sets from the company for AI based systems (especially in R&D, production, sales). This is considered a unique selling point (USP) and core know-how for future business models, for areas like predictive maintenance, digital twin.

Data of case types two and three is treated as trade secrets and is often not shared (if not negotiated otherwise with OEMs). If it is shared with the OEM, the data is not considered as a trade secret anymore (although covered by NDAs; an NDA alone is NOT considered as appropriate means to cover a trade secret if/once shared). The tier1 supplier is in this context always depending on the purchase and bargaining power of OEMs.

Typical situations for automotive suppliers to share their confidential and commercially valuable data are:

- OEMs target data as a priority and try to secure access to data (of suppliers and supplied parts and systems). However, this happens, for the moment, without the OEM fully knowing the later/future use and applications of the related data. It is more a preparation for future business models (a unilateral approach from the side of the OEM).
- Data from operations (e.g., from component in a car) is sought. So far there has been no (bilaterally) shared data for the benefit of the 1st-tier supplier (due to lack of interest or opposing interests of the OEMs). As an example, the additional use of cam sensor-based data from car operations is solely managed by OEMs and not shared with the 1st-tier supplier even if the supplier might be able to provide additional value or improved/novel business models.

As regards ways of how the firm determines whether internal data (data owned/created in-house) is confidential and commercially valuable, it was reported that all data has to get classified (by each internal function and expertise/data owner) but such classification has, however, operational limits. It was said that in the automotive supplier industry the conditions that need to be considered when sharing confidential and commercially valuable data are primarily set by the OEM on a unilateral basis. From an international perspective, specific issues arise when confidential and commercially valuable data is shared across borders in the sense of where the data originates from and where the data is stored (which leads to the question as to which legal regime is applicable).

Concerning breaches and the afterlife of shared confidential and commercially valuable data, the company reported that if data must be shared, e.g., with OEMs, the data is not considered, as stated before, a trade secret anymore. Knowledge of data afterlife use, e.g., which takes place at/with OEMs, is very limited or even non-existing. Other issues that that the firm thinks need to be considered include the link between the different data sets and the various contracts (which are mainly internal challenges); and the notion that contractual parties should decide on availability, sharing and use of data by themselves, rather than being obliged to share.

Case Study Nr. 4: Pharma firm and its need to combine forces and share data with others so that novel treatments can be created

Sector:	Health / Pharma
Type of organisation:	Large firm
Type of data shared:	Clinical trial data, molecular data, manufacturing data
Data shared with:	Research partners, competitors
Use of trade secrets:	Yes

The firm in this case study is a large pharma firm.

In terms of data of interest for sharing, the company looks at all kinds of data. The data is obtained through research and commercial activities and is needed for the firm to be (more) innovative. To that end, there is a need to engage also with patients and health care providers. The major tool of protection is trade secrets implemented via contracts. There is considerable potential for data sharing and at the same time there is also a lot of value in the data and at stake. A crucial question is how the firm can fulfil the obligations to society while protecting the legitimate value of the data for the company.

The data in focus of sharing is health-related data: clinical trial data (obtained in an "artificial" set up), real-world data (outside of the "artificial" set-up); molecular data (in the broadest interpretation: exchanged data on compounds / from combo studies), manufacturing data (when data with partners from manufacturing is shared). This data is clearly confidential and/or even highly confidential. There is hence a considerable number of data domains. The challenge is to harmonise the data and transfer/share it in secure ways (e.g., with a third party). In doing so, there is also the need to cater for the interest of the third parties (with research partners, for example, their need to publish results; there are hence also timing issues to be resolved (when one is allowed to publish)).

Peculiarities arise in relation to the development of new compounds and new analytical tools. When the company starts to develop a new compound, there is the need to collect data on the physical characteristics. There are assays to characterise the physical properties, but these need to be harmonised and calibrated, so that the assays are reliable. To achieve this efficiently with huge amounts of data this requires machine learning and AI, which is a new trend, and these methods also need large amounts of data so that they are trained. There is hence a need to mine datasets brought by many partners, and this is only possible through the sharing of data. Using these new AI/ML tools makes the company more efficient, and hence "data is gold".

There is a hence also need to get access to data also from third parties for the new tools. For that, there is also the need to have a safe environment where the company can safely share its data without disclosing its compounds and know-how. At the moment, the systems of data sharing do work, but it is highly important that data sharing remains voluntary.

Examples of data sharing practices include the following:

- First, the company shares pre-clinical data and clinical trial data. This data is stored on the company´s own platform. The access is provided to the data via an agreement for specific purposes.
- Another example is through IMI initiatives where the initiative brings different firms and universities together to produce tools, and where the company contributes with data. Based on the data, new algorithms and tools are developed that serve the whole industry. The data sharing is voluntary for this specific purpose.
- There are also instances of bilateral agreements with data providers.

- One specific area of application is predictive algorithms for the properties of the compounds which speeds up development time and may reduce the need for animal testing. A research organisation, for example, attempts to develop a tool to predict the expected survival time of transplanted organs. To this end, there is a need to mine / re-use different sets of (already performed) clinical trial data created by different firms over time.
- Another example is platform studies where there is co-development taking place with regulatory authorities (FDA/EMA) on different arms of the platform. For example, in cancer treatment R&D, a patient might not respond well to one treatment but could possibly respond well to others. In such a case, data sharing is agreed with the FDA/EMA directly- the patient could switch from one treatment option to a more fitting one, and the data is shared among the participants. This speeds up drug development, and there is an all-in-one solution from the point of view of patients.

The given examples and practices are mostly "one-off" agreements for specific data and specific purposes. One future scenario could be in very open platforms where data sharing for a pool of data is continuous with no specific purpose defined in advance – but this scenario is highly problematic, because there may be no negative repercussions for parties misappropriating the data, particularly in unforeseen ways, where the company eventually also loses control over its own data.

Concerning the protection measures and the role of trade secrets (motives for trade secret protection), the following can be said:

- Contractual measures have been the gold standard in the industry.
- Access to data is via technical means, under specific conditions and for specific data.
- Good governance processes are also a must.
- The role of the trade secret is first that of a fallback option / safety net. In contracts, it is usually defined what the confidential information is. The problem with data is that its value may not be immediately visible. The trade secret can help in situations where there is no absolutely clear-cut situation in the contracts.
- The trade secret hence works more in the background. It is also sort of a link between private law (contracts run under private law) and public law (which is trade secrets). Sanctions can be made both in relation to private (contract) law and public (trade secret) law. The trade secret is an additional means for recourse, an additional resource.
- Particularly through its use in the context of patenting, "trade secrets" define a common language (everyone understands what is meant by it, and there is hence sort of guidance on how trade secret protection works).
- In a highly regulated area like in the pharma industry, an additional benefit is in relation to freedom-of-information requests. If such requests materialise, information can be "blackened" citing trade secrets as reason.
- A specific role for trade secrets is in the context of non-intentional data sharing (so far, the instances of data sharing have been intentional): For non-intentional data sharing, trade secrets can be the last catch to protect the assets. This is a very common situation.

Concerning the barriers for trade secrets, the following can be said:

- The concept of trade secrets is still somewhat vague and ambiguous at the same time, not tangible enough. For example, what are the exact "reasonable steps" that need to be taken to "adequately" protect the data and trade secrets? The question is not yet developed in case law. It may well be that one loses trade secret protection because custody for the data is improperly given to 3rd parties.
- It is also important that the different purpose(s) of data sharing can be clearly catered for. The example of Covid exemplifies that there is big interest in data sharing for clinical end-point data, standardised test procedures etc. However, for specific know-

how on the molecules of the company there may be legitimate reasons to have some information not widely disseminated – at the same time, the company may also benefit from the sharing of data.

- There needs to be the possibility to check that the company can only share data for specific purposes and no other purposes, because the data is also used by the company itself to develop (and patent) products. The company wants to share, but voluntarily, and underlines that it cannot give everybody access for every purpose.

The current system for trade secrets seems to work OK, and there is no need to fix things that are not broken. For unclear issues it is advisable to wait for the case law to develop. Guidance for some rather ambiguous concepts ("reasonable steps") could help already, particularly in relation on how to deal with one´s own employees. There is need for good governance processes for trade secrets – this should be ensured also in initiatives like in the European Health Data Space. When hacking becomes more common, enforcement of trade secrets should be made easier (in Europe, there is very little experience with trade secret enforcement, case law needs to develop).

Case Study Nr. 5: Insurance company – heavy in data sharing, light with IP and trade secrets

Sector:	Financial Services
Type of organisation:	Large firm
Type of data shared:	Various
Data shared with:	e.g., health care organisations
Use of trade secrets:	No (of minor importance)

Insurance companies are generally data-driven companies. The entire industry thrives on knowing the risks of policyholders better than the policyholders know them themselves and using this expertise for product design. Policyholder data (personal data about the policyholder and the customer's previous activities or product use) and external data are essential for the calculation of the products and are incorporated into the product design and the business model.

Data is often shared with third parties. These are, for example, intermediaries, brokers but also other insurance companies and regulatory authorities. However, data is also shared with hospitals in the case of health insurance and in the fight against fraud, shared databases with the insurance association play a major role.

When dealing with confidential and commercially valuable data, it is important to divide the data into categories. For example, a distinction is made between General Data, Confidential Data and Strictly Confidential Data. Specific confidentiality levels are set for each of these forms and technical safeguards and contractual elements are defined accordingly. There is no standardised process for identifying confidential and commercially valuable data.

Predominantly machine-generated data (for example analyses of previous product use, frequency of claims with certain customer groups or previous commission models) is shared (e.g., insurance companies share healthcare providers in the case of medical insurances), in individual cases also human-generated data such as commission calculations. Normally Data is stored in clouds before it is passed on. Here, an explicit cloud strategy is required in which it is specified which criteria are to be adhered to here so that a cloud can be classified as trustworthy.

When purchasing third-party insurance, the data is integrated into the company's own systems as far as possible. An exchange of confidential and commercially valuable data also takes place in the following case: Insurance business runs under the label of company A, but is completely calculated and processed by another insurance company (company B).

Another scenario of data sharing for insurance companies is the opening up of new sales channels, e.g. car dealerships brokering liability insurance or automobile clubs brokering travel insurance.

The following scenario is becoming increasingly important: the insurance company identifies useful data held by another company (other insurance company but also e.g. health facility) and asks for access to this data in order to use it for its own business. With personal data, this is not so easy from a GDPR perspective, e.g. health data cannot be sold so easily, but in the future: aggregated data will be bought and analysed to derive valuable information about (customer) behaviour.

Contractual conditions for the exchange of confidential and commercially valuable data are usually adapted to the intensity and duration of the business relationship in customised contracts - e.g. for service providers. Regarding the future handling of confidential and commercially valuable data from external sources, it becomes increasingly clear that AI will be used as a supporting tool, e.g. in the analysis of error sources around errors that occur in the core-processes of insurance companies. In any case, however, a review is carried out in advance to determine whether it makes sense to use AI here. AI is not yet used as much in the execution of core processes, not as much for performance processes, but increasingly in the analysis phase AI will be used in a supportive way.

When confidential and commercially valuable data is exchanged across borders, the legal requirements in the recipient country must be met. When data is exchanged, the categories of data (categories of data processed, categories of recipients, categories of data subjects) must be identified to ensure unambiguous classification. For example, when describing the categories of recipients, care must be taken to ensure that verification of lawfulness is possible. This is very complex due to the different legal bases and very costly for insurance companies. In principle, a very restrictive approach is taken when sharing confidential and commercially valuable data, and only absolutely necessary data is exchanged with business partners, but also with regulatory authorities. Finally, patents, copyright, database rights and trade secrets for the protection of confidential and commercially valuable data are of minor importance to insurance companies or are not seen as relevant for this insurance company.

Case Study Nr. 6: Mobility service provider in the automotive sector and its use of trade secrets for protecting dynamic data and fundamental rights

Sector:	Automotive (mobility services)
Type of organisation:	Large firm
Type of data shared:	Location data
Data shared with:	Maps data suppliers
Use of trade secrets:	Yes

The case study at hand is about a firm offering mobility as a service (ride-hailing, food, delivery, package delivery, couriers, etc.). It is also known for investing heavily in R&D regarding autonomous driving.

The major type of data for which sharing is of interest is location data. Such data is acquired from smart phones (i.e., mostly machine-generated). The data could support, for example, city planning by helping to understand the behaviour of riders when they move around. The location data on movements resulting from one individual trip maybe hereby not be of so much interest but aggregating the data and observing it over time will reveal interesting patterns. By its nature, such location data is personal data which however can be in principle transformed into non-personal data through abstracting – for example, by leaving out start and end points of a trip. This procedure to obtain derived data is not perfect though. A case in point is less densely populated areas where leaving out start and end-points could eventually still lead to the identification of movement patterns of individuals identifiable by name through contextual analysis.

Given the potential for exploitation of the location data, there is demand (e.g., from city planners) for the company to share the data. These demands could be technically met by a variety of channels, including FRAND licensing arrangements; through a marketplace; and/or through (forced) regulation. Location data is hence of principle economic value, it is secret and protective measures are taken by the firm to keep the data secret. Following this, such data is trade-secret protected, particularly if it refers to the derived/abstracted data where GDPR does not apply anymore. In this context, a principal argument of the company regarding the utility of trade secret protection is that trade secrets then help secure human rights for both riders and drivers using the firm offerings – if data sharing is not well governed, there is the risk that personal data is revealed (re-engineered through said contextual analysis) and potentially abused by a third party.[205] Regulating access through trade secrets may provide hence a shield for human/fundamental rights of individuals and/or groups of individuals. Against this backdrop the company states *"…that for any mandatory regulations legislators should take a very careful approach catering for the contextual factors, which is very difficult"* (interview), so the company clearly favours voluntary data sharing governed by contracts.

Another consideration for trade secrets is the aggregated data and analysis models created by the firm using self-developed software and AI tools – one foundation of the company and a value creator. The respective tools and associated data lead to enhanced service quality such as a better matching of riders and drivers based, e.g., on personal preferences or on time-optimised routing. The company would like to consider these tools also as trade secrets. However, there are tensions with transparency obligations – i.e., documenting how the service of the firm works for GDPR purposes. The company has hereby to walk a delicate line between offering sufficient information to serve the GDPR rules and informing clients while not revealing essential information to competitors who could copy and free-

[205] However, it should be noted that this stance has been also met with scepticism. The main argument is that either the GDPR (or other data protection/ privacy rules) apply and data protection/privacy is secured, or it does not apply because there is no personal data (and in that case there is no problem).

ride on the R&D investments made (and hereby threaten the existence of the firm). Trade secrets act here as substitute for software patents which are legally not allowed.

Third party IP rights – and here again trade secrets, but also database rights – are implicated in this case, mainly those of map makers. Their know-how (and IP) is needed to turn GPS coordinates into actual addresses. A major part of the value offering of map makers is that they keep the maps constantly up to date, i.e., as high-quality dynamic data. This requires constant investments. The company sees this aspect also as the prime reason why free/open map data (even if created and offered by government) can never reach the quality of the data and offerings of private map providers.

Against this backdrop, trade secrets also help shield and monetise investments of map makers in the interest of the mobility service company as a client. Consequently, in the context of such dynamic data, trade secrets are a facilitator, even enabler, of data sharing between firms, *"…enabling others to build offerings on the shared data"* (interview). The company therefore opines that future legislation dealing with data sharing should follow the model of the GDPR which sets out limits should the GDPR infringe on the (IP) rights of others. Equivalent clauses should be copied also into other pieces of legislation, and it would be beneficial, if it is explicitly spelled out that trade secrets are an example of such (IP) rights of others.

Case Study Nr. 7: Machinery firm in the automotive sector using trade secrets as default protection measure and highlighting the subtle differences between shared confidential data that is trade secret protected and shared confidential and commercially valuable data that is not trade secret protected

Sector:	Automotive sector (supplier)
Type of organisation:	Large firm
Type of data shared:	Production process data / machine-generated
Data shared with:	Clients, research partners
Use of trade secrets:	Yes

The company in this case study is a manufacturer of machines with which high-tech components for use (also) in cars are created. These machines produce large amount of data (also including image data from cameras) which is needed to control the machines and to optimise production processes in client factories. Even small improvements here can translate into considerable commercial gains, e.g., in terms of cost advantages by managing wear and use of the machines and ensuring quality output. The data under consideration is hence mostly sensor-generated data with no nexus to personal data.

While there is therefore a clear motive to share data between firms, data sharing has so far remained a rather difficult task. Client firms fear for their own trade secrets and confidential data, and while they are interested in improving their production processes, they often do not reveal important data (e.g., in relation to quality control) which could lead to respective improvements. Clients also demand full access to all data of the machines, which is conversely also provided only partially by our case study company. Hence, there are typically tedious negotiation process in place to regulate data access rights and the modes of data sharing (such as certain data being shared only offline) with contracts. The fact that the customers are (large) firms and not consumers, however, *"…is at least somewhat simplifying things"* (interview). Nonetheless, the topic of IP and data sharing is *"…a hot topic which is currently developing in our industry."* (interview).

There are organisational and managerial ramifications of the confidentiality obligations arising from the said negotiations as "…each piece of information given to us by our clients cannot be passed on." (interview). This also applies to information flows within the firm – there are separate accounts for each client, their contact persons and liaisons must be different and business operation/contacts are also kept organisationally separate. As the R&D department operates as a central unit, information from different customers eventually makes its way to overall improvements of the machines which benefit the whole client base. The increasing need for data sharing has also rather recently led to the IP department becoming also responsible for data (sharing) from a legal point of view, with an ensuing work division that the IP department, in an iterative process, defines company-internal processes and the IT-department is tasked with implementation (e.g., through software, cryptography).

Apart from collaborating with clients, there are also collaborations with partners from research (universities, RTOs) and companies who do contract research (and produce components/parts which are only usable by the case study firm). In these instances, data sharing also takes place. There is, however, no collaboration with competitors taking place. In the context of cross-licensing agreements, though, data sharing becomes a topic as data becomes an asset in the IP portfolio in the form of data pools.

The company explains its protection strategy for shared data by explaining that the default mode are trade secrets*: "Everyone owns its data, protected through trade secrets, and data is prima facie not to be shared. Contracts hereafter soften this situation and create the exceptions and conditions by which specific kinds of data are then shared and exploited – a situation like deer hunting, where the deer can only be hunted in one´s own woods,* *even if the deer moves freely between different woods."* (interview). This means that trade secret protection and access to them is applied through contracts. In addition to trade secrets, the firm makes heavy use of TPMs of all kinds. Apart from data being subjected to trade secret protection, trade secrets are also an important means to protect the Machine Learning algorithms used to create derived/processed data.

Interestingly, the company reports that the industry often does not differentiate well between trade secrets and confidential information. Single data is not commercially valuable (hence not trade-secret protected), but the complete data, the "*whole picture"*, is of value. Similarly, original data is not (that) valuable, while data derived/processed from the single data has significant value. The distinction between confidential information and trade-secret protected data is, for the firm, however subtle and critical at the same time. The major point is that both types of data/information are and should be protected, but only one of them enjoys the additional trade secret protection. Great care must be taken to also protect the original (confidential) data: "*Trade secrets and confidential data are theoretically something different, but in practice both should be managed the same way."* (interview).

The possibilities and limits to enforce of trade secrets is a topic that is hotly debated in the industry, but the company has so far had little problems. The major concern are employees which leave the company, while industrial espionage is hardly visible. A certain base level of "industrial espionage" is said to be unavoidable, as clients share parts of presentations with competitors or, if they bought a machine, show it and ask questions like whether the case study firm machine can do the same or be developed to do the same as the competitor machine. In practice, hence, companies *"...need to walk a fine line between showing/sharing and keeping things secret, otherwise follow-on innovations are not possible."* (interview).

Finally, the firm would welcome if the EC created Directives and rules for trade secrets and data sharing and leads respective developments, as the experience of the firm is that the EU enjoys role model character in this regard (particularly in Asia) and hence European principles could find their way into other legislations, hereby facilitating trade and data sharing.

Case Study Nr. 8: OEM firm in the automotive sector stating that data sharing follows investment principle and is not available for sharing "as such", while also raising antitrust issue as a barrier to confidential and commercially valuable data sharing and trade secret usage

Sector:	Automotive sector (OEM)
Type of organisation:	Large firm
Type of data shared:	Various
Data shared with:	Suppliers, partners from other industries (insurance companies)
Use of trade secrets:	Yes

The firm in this case study is an EU based automotive OEM. Currently, confidential and commercially valuable data is shared based on stand-alone license agreements and as integral part of broader agreements. Currently, NO data is generated and processed without purpose, since the generation and processing of confidential and commercially valuable data requires significant investment. Therefore, the efforts necessary to generate and process data that is then "ready to share", have to be evaluated from a business perspective, in particular, a return-on-investment perspective. Currently, NO data is "just available" without any prior investment.

In five years, it is highly likely that there will be more investment in the generation and processing of data in the automotive industry and more data will be used. Data is shared – as licensor and/or licensee – based on contracts. Typical scenarios or partners are, e.g. (a) suppliers (patent and know-how licensing agreements), (b) cooperation partners (e.g., with insurance companies), (c) integration of digital services (e.g., with the GAFA actors), (d) service providers in the after-market, (e) compulsory licence schemes, e.g., based on EU type approval regulation, (f) "classic" technology transfer agreements (under TTBER license agreements). Confidential personal data is constantly shared upon request/explicit permission of end customers, e.g., customer wants to share data with its insurance company.

Typical motives to share confidential and commercially valuable data are to establish a common basis for partners to create better innovations. Sharing of data on a bilateral level generally happens to create value on both sides, i.e., there is no selling of data as such (at least not yet as there are no markets). There is always own business purpose (but only if it is legally permitted to share, e.g., due to antitrust laws). There are also typical reasons (barriers) not to share confidential and commercially valuable data: confidential and commercially valuable data is considered as trade secrets and confidential know-how, which is of strategic relevance and can, therefore, not be shared from a business perspective and/or an antitrust perspective.

"Technical" bottle necks (e.g., data is not available "ready to share", e.g., also from a data protection perspective) and legal uncertainty (data protection, antitrust laws, no clear IP protection, etc.) are by far the biggest obstacles for sharing of confidential and commercially valuable data. Often, limited return on investment but high (legal) risks and administrative expenses. Typical data type dimensions of shared data are machine-generated-data vs. human-generated-data, non-personal data vs. personal data as well as static vs. real time data

Besides the sui generis protection of databases, trade secret protection (under the EU TS Directive) is the second statutory pillar for protection of confidential and commercially valuable data for innovative companies. These two legal means are, next to the contractual means, most relevant for handling the sharing of confidential and commercially valuable data; trade secrets and database protection are the legal basis for justification of certain data licensing agreements, in particular, justification of, for example, "field-of-use" restrictions, that in consequence foster data sharing; trade secrets are therefore a very relevant instrument for secrecy and know-how protection.

Typically, contractual and legal measures are undertaken to protect confidential and commercially valuable data. However, these measures are not considered to be adequate in face of the risks associated with the loss of secrecy: Trade secret protection does not allow for open-data-initiatives, since "open" data sharing will automatically end trade secret protection. Unlike open-source-initiatives, where software copyrights provide a clear IP framework, IP protection (sui generis right for database protection) for data is relatively limited, and its scope of protection is not entirely clear.

The firm states that adequate protection of investments is key for innovative businesses. The willingness to share confidential and commercially valuable data is directly related to the level of protection for confidential and commercially valuable data holders and a clear legal framework. Only if the current level of protection for confidential and commercially valuable data under the database directive and the TSD will be maintained and further developed to adequately protect the investments associated with the generation and processing of data, innovative businesses will become more open to share confidential and commercially valuable data. Without sufficient IP and know-how protection, most businesses will simply rely on and maintain the secrecy of their confidential and commercially valuable data.

The firm believes that the scope of protection of the sui generis right for databases is relatively limited and should be broadened and clarified, including machine-generated data and investment in the creation/generation of data (as this is currently not clearly covered by the legal regime in the EU). Concerning breaches and the afterlife of confidential and commercially valuable data shared, it was stated that breaches do occur quite often and are triggered by limited IP protection and burdensome enforcement of trade secrets.

The firm noted, eventually, that several EU initiatives try to encourage businesses to share confidential and commercially valuable data which obviously consist of confidential and commercially relevant information. At the same time, though, the exchange of such information between certain businesses is a major antitrust issue (see horizontal guidelines). The question therefore remains for the firm of where the EU wants to draw the line.

Case Study Nr. 9: A banking federation in an EU member State reporting on various data sharing practices, the big issue of personal data protection and the little (but growing) role of IP and trade secrets

Sector:	Financial (banking)
Type of organisation:	Association
Type of data shared:	M&A data, data to detect crimes, R&D data
Data shared with:	Banks, insurance companies, tech firms
Use of trade secrets:	Not uniform across sector

Data protection issues, and less so trade secret considerations, often inhibits sharing considerations between banks. There is a general reluctance in banks to share data with other companies. Advantages through joint data sharing are an important point of discussion. One advantage is seen in the increase in efficiency through data sharing; the current data protection framework is considered too narrow and contains too many legal provisions from the banks' point of view. The partly very old systems in banks for customer master data pose a particular challenge. Data transfer and cloud issues are highly relevant, especially regarding the server location. The servers should in any case be in an EU country; a location in the USA is seen as very critical and is often ruled out.

Basically, questions often arise such as: What services can a bank develop beyond the traditional banking business - what additional data will be used here? Will the new service be offered on the market independently or with cooperation partners? This is still a very new area, but it is developing dynamically, and the use of AI will certainly play an important role here in the future.

Reasons for not sharing confidential and commercially valuable data are often a wait-and-see attitude on questions of expected technological development, but also a critical discussion about the value of shared data and possible risks associated with it.

Joint projects increasingly play a role in banking and are therefore very relevant, here data is also generated jointly by several actors. Data exchange is an issue both within the banking industry and also with insurance companies that are closely linked to banks and with the public sector, but increasingly also with technology corporations. Typical situations in which companies share their confidential and commercially valuable data (or intend to do so) are, for example:

- Mergers and cooperation with other financial service providers. In advance, however, it must be clarified how the partner fits in with the company in terms of business policy, then in a second step the joint use of data is negotiated and agreed.
- Shared data is also used, for example, for transaction monitoring to detect potential crimes.
- Data is also shared with universities for scientific projects for example, when industry studies are prepared.

Customer data is very valuable for future business models and raw data from various internal and external sources is used here. For example, this data is used to train AI models - this aspect is becoming increasingly important. Technology companies more and more want access to banks' data, but should also share data, this is already being done today in individual cases, but it will certainly become more important in the future. Synergies from data use are increasingly relevant for business model development.

For many projects, data sharing would be beneficial, but the data protection framework contains a lot of provisions, especially regarding the protection of personal data, and the banks act very cautiously here. A particular area of tension is seen in scoring models: the method and parameters are not to be disclosed, but on the other hand consumer protection groups often demand that customers be able to recalculate their score. An intensive exchange of data takes place with the regulatory authorities. When AI is used to fulfil supervisory obligations, the regulatory authority wants traceability.

Technical security is indispensable for the protection of confidential and commercially valuable data. The protection of the entire infrastructure is therefore particularly important. In the event of the loss of confidentiality of data, the speed of reaction and the development of defence capabilities - here in particular the training of experts - must be emphasised.

In the international exchange of confidential and commercially valuable data, it is particularly important that the role of London in the financial market could not be substituted in the past. Within the EU, the standard of data protection is considered high; the situation with the USA is seen as more problematic; here, corresponding contractual clauses are very important.

Patents, copyrights, database rights and other IP rights for the protection of confidential and commercially valuable data currently play a rather minor role for the financial industry, but their importance is expected to increase in the future. There is no uniform view among the banks on the future importance of trade secrets as a legal tool, and the assessment of the future importance also varies greatly across the industry. With the increase in cooperation, also with companies from outside the sector, the importance will possibly increase.

Case Study Nr. 10: A bank with lots of confidential and commercially valuable data sharing, use of contracts but no real use of trade secrets

Sector:	Financial (banking)
Type of organisation:	Bank
Type of data shared:	Company investment data, software code
Data shared with:	Banks, insurance companies, tech firms
Use of trade secrets:	Not uniform across sector

The firm in this case study is in the financial business, with headquarters in Switzerland. It operates in the U.S., Asia, Japan, Europe, and the United Kingdom. The interviewed partner has a background in professional financial services, as employee of the R&D department of a large bank, in venture capital and as owner of a company dealing with crypto assets.

The firm has experience in the general sharing of data in the context of company investments. These confidential and commercially valuable data are protected with NDAs or mutual agreements with a confidentiality clause. In relation to the protection of software codes, normally one single person is appointed to keep the software code confidential. The company is working in finance big data clusters where it must distinguish between confidential and commercially valuable financial data. Guidelines related to data storage, data exchange, machine learning, AI and on "how to go live" are necessary to be shared by banks. Confidential and commercially valuable data will be typically shared with the national regulator.

Typical motives to share confidential and commercially valuable data are entering new collaborations – be involved in the "next level" and create dummy data for some forms of algorithms. Also, a motive to share confidential and commercially valuable data is learning to know how systems are changing related to common data exchange. There are no good reasons not to share data. according to the firm.

In the future the major issues will be machine learning and AI. Lots of data will be created in e.g., trade finance and car companies. A considerable number of standards will be created. The biggest issue will be ensuring the data-tracking and SSI (Self Standard Identity). Who owns the data will be informed about someone who looked at the data. The company is protecting the confidential and commercially valuable data contractually and with legal access only for selected persons. The motto of the firm is *"the fewer people the more secrecy"* and vice versa. Very important is copyright for the software protection.

The application of trade secrets for protecting confidential and commercially valuable data is depending on the type of data, also if there are individual data. Data are stored on an own server or in the cloud. Extremely confidential data are stored on hard disks, will be locked by a key and are not going to be stored in a cloud. The firm is very rarely applying trade secrets. Breaches have taken place but have not been brought to court right now. The big issue for the data owner is the exposure of sensitive data to third parties. Here one must evaluate very carefully on how data will be passed on and used.

The major take-away from this case is that the financial company is not using trade secrets and tries to protect the confidential and commercially valuable data with other means available for them in the financial area.

Case Study Nr. 11: Electrical and power engineering firm showcasing how to handle different levels of confidentiality while still climbing the trade secret learning curve

Sector:	Energy (utilities)
Type of organisation:	Large firm
Type of data shared:	Product part data/specifications, sensor-acquired data
Data shared with:	Universities, research institutions, companies with which collaborations are carried out
Use of trade secrets:	Yes

The following case study is about an electrical and power engineering company based in Germany. Its portfolio includes power generation, transmission and distribution (e.g., transformers, switchgear, high-voltage direct current transmission, power plant technology, low-voltage switchgear as well as turbines and compressors). An interview was conducted with a patent attorney who has been with the company since 2013.

The topic of data sharing is extremely important not only for the patent attorney who, in his role, is dealing almost exclusively with confidential data, but also for the company overall. The firm takes great efforts to keep confidential data confidential as it sees itself in a continuous process of information and data exchange.

Intellectual property issues repeatedly arise in collaborations and must therefore be regulated, respective assets protected. Very often know-how and trade secrets also arise when a data exchange is deemed necessary. Cases in point are when two companies do not work together in a development group, but each company develops a part of a product by itself. Then, information must be exchanged on key technical data, product parts, etc.

Another typical business case in a digital setting would be that in a large power plant, the power plant operator has very valuable data for the turbine manufacturer (i.e., how well the turbine operates). Data is shared with universities, research institutions, companies with which collaborations are carried out, but never with competitors unless they become partners. As the exchange of sensitive information and technical data is often part of the informal talks in the early stages of collaborations, employees are encouraged to use NDAs from the start. The core of the problem in collaborations is that it must be clear who "owns" the data as companies try to avoid generating common data and try to establish who generated the data and then delimit who owns which data.

The company also uses trade secrets as a legally defined instrument and has implemented measures as an internal company policy to protect data. Classification is done according to content and use/purpose of data (e.g., very confidential data for example can only be viewed on site). Moreover, different tools are assigned to different levels of trustworthiness. Personal data are left out and is usually not accessible at all, as it has no IP relevance.

There are policies, technical measures, encryption of emails, tools and instruments available for data protection. As confidential data can also be found in emails etc., the assessment and classification of data is done by the person who creates the information. Each employee must choose a classification and, depending on the chosen classification, select measures to ensure data security. The company considers its measures good, but not always sufficient as outflow of information has happened in the past. However, the question is if sufficient measures can even exist. To avoid voluntary and involuntary leakages, a culture of awareness is crucial. Therefore, a lot of effort and focus is put on training of employees on how to handle data appropriately.

In case of a data breach or theft happening, the company often ultimately can do nothing, apart from checking registered IP rights and hereafter taking action. Frequently, however, the time and effort to take the measures are deemed too high. To sum up, the company acknowledges the need for tools covered by the new law but admits that it still needs to be implemented and lived.

Case Study Nr. 12: Automotive supplier with strong trade secrets policies

Sector:	Automotive (supplier)
Type of organisation:	Large firm
Type of data shared:	Production process data, sensor-generated data from vehicles, product specifications and simulation model data
Data shared with:	Clients, R&D partners
Use of trade secrets:	Yes

The company in this case study is an EU based automotive supplier. The firm considers itself as a large company in general terms, but medium-sized compared to other automotive industry players, e.g., the OEM car makers. Therefore, the company cannot do everything on its own but relies on partnerships with other companies.

Sharing of data therefore typically occurs when:

- The company must share data with clients and the clients must share data with the company, e.g., business plans, company products; also sharing data with partners to have best processes and ingredients (focus: making and selling the product: tires; sold to OEMs or to traders).
- How the supplier product is behaving in the car: data on how the car is behaving
- Vehicle to Vehicle (V2V) communication (weather, road situation) – data to share with other players outside the "traditional" automotive sector, e.g., Vehicle to Infrastructure communication, autonomous and assistive driving scenarios.

The company considers the biggest challenge not to underestimate the value of the data, i.e., building business models and value with the use of data (interaction between supplier and OEM car maker, purchase, cost of components such as for sensors); there are technical constraints, but key is the value model. An example is e.g., the introduction of sensors in the supplier product ("*without it you cannot drive/use a car*"); data is e.g., pressure, temperature (of what: air, surface, internal structure); interaction with the road (friction coefficient). However, suppliers do not want to offer data for free but want to participate in the generated value (which means there is a challenge to find a common language and a win-win situation between supplier and OEM).

The company shares confidential and commercially valuable data with OEM car makers, partners, and clients. Typically, the motives to share confidential and commercially valuable data are related to the development and production of the supplier products. Typical reasons and barriers not to share confidential and commercially valuable data are, e.g., if there is no understanding of the business model for the use of the confidential and commercially valuable data.

Sharing of confidential and commercially valuable data takes places either bilaterally or unilaterally when this is necessary – e.g., for the development and production of tires, including simulation data, data on ingredients. Provided or exchanged confidential and commercially valuable data, including know-how, is generally considered to be trade secrets. Much of such data is structured and classified in internal data bases.

The standard scenario for confidential and commercially valuable data sharing occurs during the development and production of the firm´s supplier products: The OEMs provide the supplier with the necessary data to design and produce a new supplier product (a "*…usual and established business*" (interview)); the supplier in turn provides data such as parameters generated from their simulation models (supply product simulator – car simulator). Confidential and commercially valuable data is kept confidential within bilateral (data exchange) or unilateral contractual legal frameworks.

The company considers its industry sector generally to be more cautious in their handling of legal and physical assets than the level provided for by the law (which refers mainly to trade secret laws). Consequently, the company classifies in rather rigid manners what is a real "trade secret" for them and what is not and applies legal and physical measures to protect the know-how and data. The firm therefore identifies interesting data assets by classifying certain information types, e.g. production know-how, that is "confidential". An issue with this kind of classification would be if a decision is taken that data is NOT a trade secret but if the decision later proves factually to be wrong (as every piece of information could be valuable). The firm conducts risk an assessment of what is known vs. what is not known.

Sharing of data is, as stated before, generally protected by contractual agreements (bilateral or unilateral): everything exchanged IS know-how and data (internal data bases with different access levels) and IS to be treated confidentially by default, unless it is proven that it is public.

From an international perspective specific issue arising when confidential and commercially valuable data is shared across borders are, e.g. when selling production machines to China (sold by piece, but including necessary confidential and commercially valuable as part of running the machines); replication of machines and flooding of market with re-fabricates of lower quality from that machines (which is a business issue rather than legal issue). According to firm, the harmonization of the international laws and national/regional laws go in the rights direction.

Other issues that on behalf of the company that need to be tackled:

- Future scenarios: The assessment of value and reimbursement for common access to data is still an open issue. However, first, there needs to be the understanding that the data has value.
- Open access scenarios need to be differentiated: One needs to get something in exchange, e.g., commons, but what is exchanged has still to be understood and agreed upon.

Case Study Nr. 13: Health business running a data trade business and applying trade secrets with different levels of confidentiality

Sector:	Health
Type of organisation:	Large firm
Type of data shared:	Various
Data shared with:	Various
Use of trade secrets:	Yes

The company at hand is in the health business and operates worldwide. The interviewed partner has a background as PhD Chemist and German and European patent attorney and is heading the patent department.

The company´s main business is getting the data for analysis to the internal server from customers and give it back after analysis and processing to the customer. The firm operates hence in an area of a data exchange, whereby confidential and commercially valuable is processed, personal data as well as business data. The stock exchange data comprises, more specifically, sales data, business results and profit warnings. Personal data are HR-data and inventor data. Inventions, know-how and clinical data are belonging to data within the scope of business activity. Certain data from clinical trials may not be shared.

Confidential and commercially valuable data will be shared with customers and suppliers on a contractual basis as NDAs, collaboration agreements, contract research agreements or contract development agreements. The company is dealing with confidential and commercially valuable data, which do not depend on persons, business data and relevant data from tests and test devices for medical use and approval of drugs.

Typical motives to share confidential and commercially valuable data are economic reasons, profit, prestige, and goodwill. The reasons not to share confidential and commercially valuable data can be legal reasons or certain confidential data from clinical trials that must be kept confidential. Also important for sharing confidential and commercially valuable data or not is the fact how trustworthy the customer/client is for the company. Currently, the firm is already sharing confidential and commercially valuable data on a regular basis. In the future sharing confidential and commercially valuable data will become more and more important and data trading can also play an important role in the development and growth of their business.

How is shared confidential and commercially valuable data protected? First, there will be an evaluation of the confidential and commercially valuable data which results in a classification in public data, confidential data, highly confidential and top-secret data. The confidential and commercially valuable data exchange will then be regulated between the company and the customer/client with the relevant contracts, set on a case-by-case evaluation. Due to different regulations and laws in different countries, EU data will, for example, stay on EU servers and U.S. data will stay on U.S. servers.

Trade secrets are having an important role for the company. The confidential and commercially valuable data will be kept confidential for protection against competitors. Confidential and commercially valuable data will be handled as trade secret due to legal obligations, e.g., patient data. Also, mergers & acquisitions data will be kept as a trade secret as well as confidential and commercially valuable data of Joint Ventures.

The takeaway from this case is that confidential and commercially valuable data is becoming increasingly important for business in today's digital world. In the future, one can very well imagine building up another pillar with confidential and commercially valuable trading in the health business.

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);

- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries
  (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm)
  or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

Priced subscriptions:

- via one of the sales agents of the Publications Office of the European Union
  (http://publications.europa.eu/others/agents/index_en.htm).

EA-09-22-449-EN-N

Publications Office
of the European Union