



The Alliuris Legal Lab

# Legal Management of Digital Aspects

Herfurth & Partner | Hanover | October 2022

**ALLIURIS LEGAL LAB  
by Herfurth & Partner**

Organisation & Conference Management:  
Alisha Daley-Stehr, Alliuris Hanover / Brussels

Editors & Lecturers:  
Ulrich Herfurth, Rechtsanwalt  
Antonia Herfurth, LL.M., Rechtsanwältin,  
Sara Nesler, Mag. Jur. (I), LL.M.  
Herfurth & Partner, Hanover / Brussels

Concept & Supervision:  
Ulrich Herfurth, Rechtsanwalt,  
Herfurth & Partner, Hanover / Brussels  
Alliuris Chairman

*With special thanks to*

Prof. Dr. Andreas Wiebe, LL.M. (Virginia) Program Director  
Andriy Ilyuk Academic Coordinator  
of  
LIPIT Master Study Course  
Georg August Universität, Göttingen

---

Published by ALLIURIS A.S.B.L.  
Avenue des Arts 56,  
B-1000 Brussels / Belgium  
Fon ++49 511 30756-0  
Fax ++49 511 30756-10  
Mail [info@alliuris.org](mailto:info@alliuris.org)  
Web [www.alliuris.org](http://www.alliuris.org)

Editor: Ulrich Herfurth  
Layout: Alliuris

# The Alliuris Legal Lab

## Legal Management of Digital Aspects

Herfurth & Partner | Hannover | Oct 2022

# ALLIURIS LEGAL LAB

IN COOPERATION WITH THE UNIVERSITY OF GÖTTINGEN  
HANOVER, SEPTEMBER – OCTOBER 2022

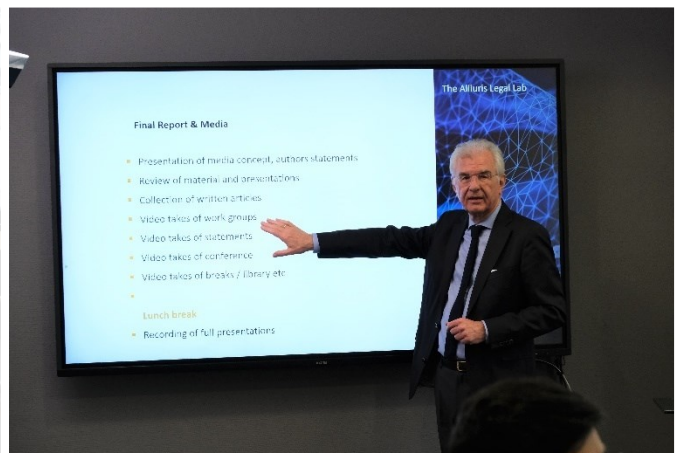
## HANOVER

HOSTED BY  
HERFURTH & PARTNER, HANOVER





Andriy Ilyuk, Sara Nesler, LL.M. (Münster) and Antonia Herfurth, LL.M. (Göttingen) (upper row)  
Professor Dr Andreas Wiebe, LL.M. (Virginia) and Ulrich Herfurth (bottom row)



## The Alliuris Group

The Alliuris Group is composed of independent, medium sized law firms in Europe, USA, Latin America and Asia, who specialise in European and international business law. The experience of the firms covers all areas of civil and corporate / commercial law to enable them to fulfil all the legal requirements of the medium sized company.

### Alliuris Academy & Summer School

One of Alliuris' goals is to promote and involve the next generation of lawyers. To this end, the members have developed the Alliuris Academy, under the umbrella of which the annual Summer School takes place. Since 2006, young lawyers from the member firms have been meeting and taking part in joint lectures and exchanging professional views. The Summer School also serves to get to know each other personally in order to build up a good and trusting working relationship. Each time, it is hosted by a different member law firm in its country.



### Alliuris Legal Lab by Herfurth & Partner

Another format to provide practical and professional information to young lawyers is the Legal Lab, organized by Herfurth & Partner in Hanover. In the Lab the young lawyers have to develop solutions for the use in the business or in companies, mostly related to digital aspects. This year the jobs were focussed on

- Data Act and impacts on SME
- Risk Management for Artificial Intelligence
- Data Compliance
- Due Diligence on digital aspects

## LIPIT LL.M. at the University of Göttingen

The LL.M. in “European and Transnational Law of Intellectual Property and Information Technology” (LIPIT) is a postgraduate Master’s programme at the Georg August University of Göttingen. The Master’s programme is integrated into the chair of Professor Dr Andreas Wiebe, LL.M. (Virginia), Andriy Ilyuk is the Academic Coordinator.

The international and English-language LIPIT LL.M. covers, among other things, the areas of national, European and international IP and IT law, data protection law and competition law. Furthermore, the economic basics of IP and IT law are taught and an introduction to legal informatics is given. As the programme is aimed at practitioners, it also includes further courses on contract drafting, comparative law and cross-border litigation. The international lecturers are selected from a wide range, such as lawyers in IP and IT law, in-house lawyers for large companies, privacy officers of multinational e-commerce companies and IT experts.

The University of Göttingen is ranked among the best German higher education institutions in various national and international university rankings. Its Faculty of Law enjoys excellent reputation for teaching, research, and professional development. Since its foundation in 1737, the University has provided excellent study and research opportunities to students and scholars from all over the world, including more than 40 Nobel Prize winners. The Göttingen State and University Library is one of the largest libraries in Germany.

For more information about the LIPIT LL.M.:

<https://www.uni-goettingen.de/en/545891.html>





Group work





## The Work Groups in the Legal Lab

### The Data Act and its impacts on SME

In their work, Aurora Mullatahiri, Özge Dülger, and Nicole F. P. de Lima highlighted some key points around *the Data Act* and its impact on small and medium enterprises (SMEs). First, they examined the definitions and concepts behind SMEs and from the Data Act, also bringing an analysis on practical applications and implications. Indeed, the Data Act has introduced remarkable legal innovations aiming to increase the data flow, the control of users on their own data and interoperability and seeking to avoiding the data dominance of bigger players in the market.

Because of the global Covid-19 pandemic, whose effects are massively felt by the local governments, the LL.M. candidates also focused on the new rules allowing a broader access of public sector bodies to data that is held by private sector entities (except for micro and small enterprises).

Lastly, they gave an insight on how the Data Act is regulating the sharing of data with third parties, its effect in practice and its influence on data deletion in general. Information was also given on some of the issues that will arise with the implementation of the Data Act as a horizontal legislation in relation with IP rights protection and competition law.



Nicole F. P. de Lima, Özge Dülger and Aurora Mullatahiri



Boğaçhan Emre Uysal and Xiao YU

### Artificial Intelligence

Xiao YU and Boğaçhan Emre Uysal, with the collaboration of Daniela Colorado, have been dealing with the topic *Artificial Intelligence* (AI). Even though AI has spread widely and has been incorporated in many aspects of our daily life, many people are still oblivious of its effects and our dependence on it. For this reason, the LL.M. candidates began their work by correcting some myths about AI, like the common worry that AI will become conscious and evil one day. Then, they analysed the real dangers associated with AI: those that could hurt businesses, customers, or have a negative impact on the society as a whole. These possible dangers could come from a variety of sources, including the data used to train the AI system, the AI system itself, how the AI system is utilised, and the AI system's general administration.

The young lawyers also provided an overview of the current legislation on AI in the USA, China, and the EU (discussing the proposed AI Act) and described the precautions to be taken in the management of AI systems. Furthermore, they pointed out the future risks associated with the outsourcing of corporate decision-making to AI and the effects of the growing automation of simple task for society and the workforce.



## Data Compliance

Eylül Gürel, Nicole F. P. de Lima, and Thiti Sriwang focused on *Data Compliance*. The first part of their work defined data compliance and described the four steps involved: the identification of risks, the creation and implementation of processes for the protection from these risks, the monitoring and assessing of the effectivity of the processes and the resolution of compliance issues. They also gave an overview of the role of the people responsible for data compliance, usually the chief data officer and the data protection officer.

In the second part, they delineated the component of an effective data strategy: first, the data should be managed in order to ensure a secure, effective and cost-efficient use. Data should also be properly collected, transferred and stored. Furthermore, data security must be ensured. In order to do this, the main stakeholder shall understand and approve the data protection strategy, a track of all available data shall be kept, and a risk analysis shall be conducted.

In the third section of their work, the LL.M candidates focused on the practical aspects of data due diligence, describing the information and notification obligations imposed by the General Data Protection Regulation (GDPR).



Thiti Sriwang, Eylül Gürel and Nicole F. P. de Lima



Mustafa Enes Balin, S. J. Jagannadh Palepu and Irem Atik

## Data Due Diligence in M&A Transactions

Mustafa Enes Balin, Irem Atik, and S. J. Jagannadh Palepu worked on the topic *Data Due Diligence in M&A transactions*. Mergers and Acquisitions represent an important tool for businesses to innovate and expand to other markets.

The Latin doctrine “caveat emptor” also applies to M&A transactions. It translates to “Let the buyer beware”, which means that the buyer is solely responsible for checking the quality and suitability of the goods before making the purchase. Similarly, the acquirer of a business must do the necessary homework on the target company, that is the due diligence which is conducted internally for the purposes of knowledge and awareness and risk analysis.

Nowadays, access to data and control over data has become a yardstick to measure the company’s presence and success in the relevant market. Additionally, due diligence must include a scrutiny of the issues related to data ownership, security, privacy, and transfers between the merging businesses. In this backdrop, the young lawyers have provided a toolkit on how to tackle the key considerations when conducting a due diligence on data related issues, IT security (including cyber due diligence) and data privacy and protection issues.



Final day with group presentations





# DATA ACT

## FINAL REMARKS ON DRAFT DATA ACT

Aurora Mullatahiki  
Özge Dülger  
Nicole Fontes Pinheiro de Lima

Visual image: <https://www.reuters.com/business/technology/ai-act-2022-10-17/>, accessed on 13.10.2022



## Artificial Intelligence: Risk Management

**AI Team**  
Xiao YU  
Boğaçhan Emre Uysal  
Daniela Colorado

17 October 2022



## M&A Transactions, Due Diligence in IT Security, Data, and Data Protection

Legal Lab, Herfurth & Partners

Mustafa Enes Balin  
İrem Atik  
S. J. Jagannadh Palepu



# Data Compliance

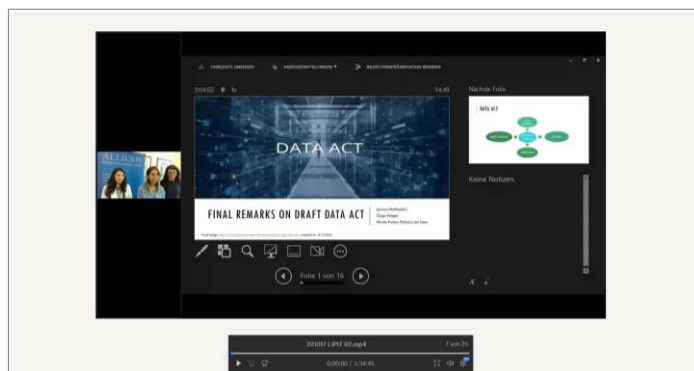
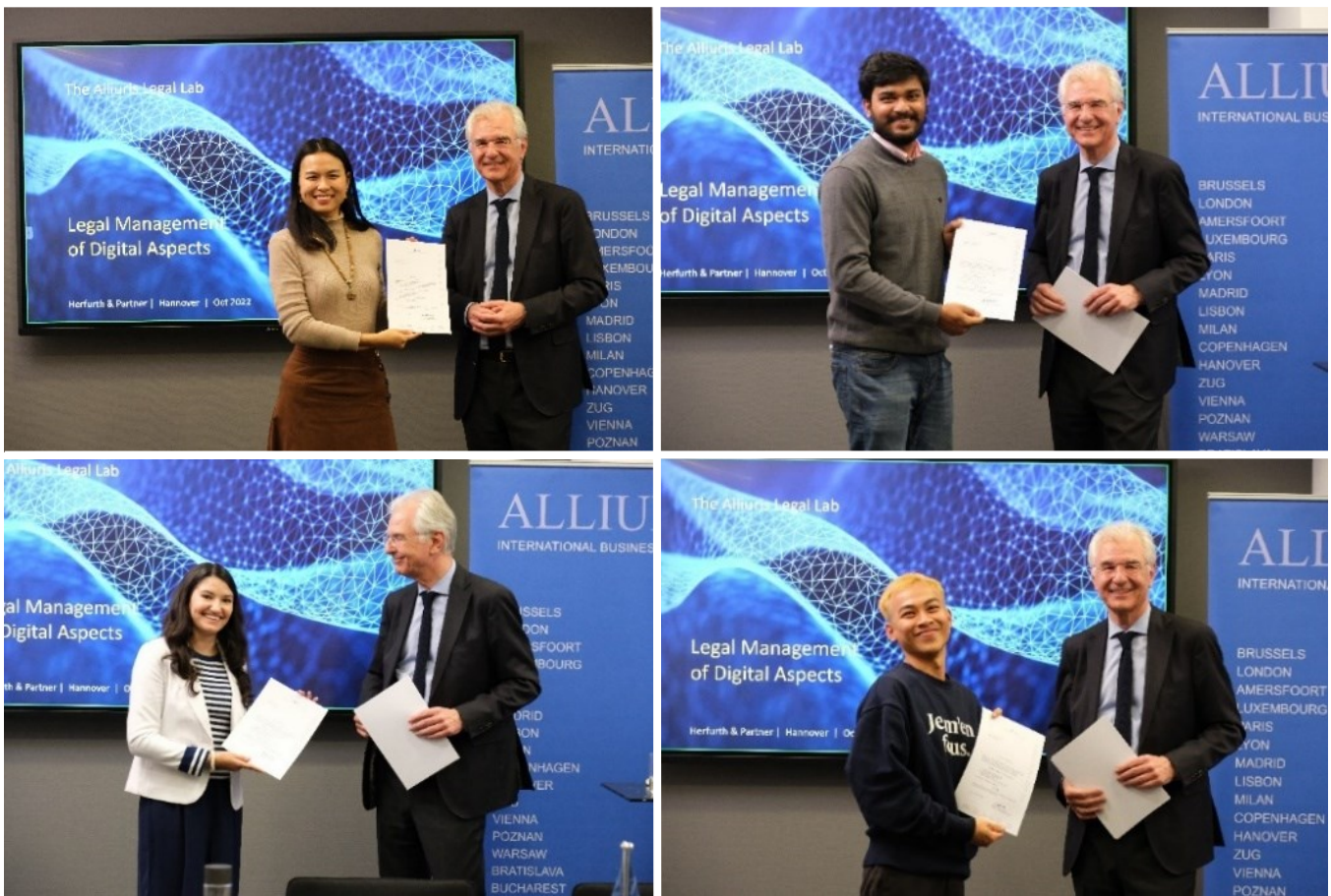
October 17th, 2022  
Alliuris Legal Lab

Thiti Sriwang  
Eyül Gürel  
Nicole Lima









Recording of the presentations



Handing over of the Certificates







The Group picture

## THE ALLIURIS GROUP

### ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

---

- 4|5|3 Lawfirm, Barcelona/Madrid, Spain
- Armstrong Teasdale, London, UK
- ATPR Sociedade de Advogados, Lisbon, Portugal
- BCO Bazán Cambré Orts, Buenos Aires, Argentina
- Brand & Partner, Moscow/Minsk, Russia
- Deustua & Halperin, Lima, Peru
- Farthouat Avocats, Paris, France
- FDL Studio legale e tributario, Milan, Italy
- Fellows Advocaten, Knokke, Belgium
- Guangdong J&J Law Firm, Guangzhou, China
- Hammurabi & Solomon Partners, New Delhi, India
- Herfurth & Partner, Hanover, Germany
- Karytinios Partners, Athens, Greece
- Key Legal, Brussels, Belgium
- LEXTRUST Avocats, Luxemburg, Luxemburg
- Marree en Dijkhoorn, Amersfoort, Netherlands
- Muheim Merz Baumann, Zug, Switzerland
- Nyborg & Rørdam, Copenhagen, Denmark
- Pacheco Neto Sanden Teisseire, São Paulo, Brazil
- VHM Vavrovsky Heine Marth, Vienna/Salzburg, Austria
- Saône Rhône, Cabinet Juridique, Lyon, France
- SMPS Legal, Mexico City, Mexico
- Yamaner & Yamaner, Istanbul, Turkey

## Imprint

Published by ALLIURIS A.S.B.L.

Avenue des Arts 56,

B-1000 Brussels / Belgium

Fon ++49 511 30756-0

Fax ++49 511 30756-10

E-mail [info@alliuris.org](mailto:info@alliuris.org)

Web [www.alliuris.org](http://www.alliuris.org)

Editors in Hanover:

Chief editor (responsible): Ulrich Herfurth

Co-editors: Antonia Herfurth and Sara Nesler

Photos: Ulrich Herfurth

Layout: Alliuris

# Alliuris Legal Lab Report

---

## Content

<b>I.</b>	<b>The Data Act</b>	<b>1</b>
1.	The Effects of the Data Act on the Practice of SMEs <i>(Aurora Mullatahiri, Özge Dülger, Nicole F. P. de Lima)</i>	2
2.	Presentation	24
<b>II.</b>	<b>Artificial Intelligence</b>	<b>33</b>
1.	Artificial Intelligence Risk Management <i>(Xiao YU, Boğaçhan Emre Uysal)</i>	34
2.	Presentation	43
<b>III.</b>	<b>Compliance</b>	<b>63</b>
1.	Data Compliance <i>(Eylül Gürel, Nicole F. P. de Lima, Thiti Sriwang)</i>	64
2.	Presentation	77
<b>IV.</b>	<b>Due Diligence</b>	<b>88</b>
1.	Due Diligence on IT, Security, Data and Data Protection <i>(Mustafa Enes Balin, Irem Atik, S. J. Jagannadh Palepu)</i>	89
2.	Presentation	104

I.

---

# The Data Act

# The Effects of the Data Act on the Practice of SMEs

*Aurora Mullatahiri, LL.B. (Kosovo)*

*October 2022*

*Özge Dülger, Attorney at Law (Turkey)*

*Nicole F. P. de Lima, Lawyer (Brazil), LL.B. (Amazonas, Brazil)*

## 1. Overview

This work aims to highlight some key points around Data Act and its impact on SMEs. This topic will examine generally and specifically the definitions and concepts from Data Act and SMEs, also bringing an analysis on practical applications and implications.

Data Act has introduced remarkable Articles that aim to increase the data flow, control of Users on their own data as well as interoperability and avoiding data dominance of bigger players in the market. After the effects of global health pandemic are felt massively especially by the local governments, also new rights to broaden the possibilities that allows public sector bodies to access the data that is held by private sector entities (except the micro and small enterprises).

Lastly, the paper gives insights on how the Data Act is regulating the sharing of data with third parties, its effect in practice and in general its influence on data deletion. In the end it provides sufficient information regarding some of the issues that will arise with the implementation of the Data Act as a horizontal legislation in comparison IP rights protection and Competition Law.

## 2. Aims of the “Regulation of The European Parliament and of the Council on Harmonized Rules on Fair Access to and Use of Data (draft Data Act)” and Definition of Micro-Small and Medium Sized Enterprises According to Recommendation 2003/361/EC

### 2.1. Data Act

The Data Act is part of a major “*European Data Strategy*” presented by EU Commission, being a relevant step for a more innovative data economy. The draft of legislation tries to ensure a fair distribution of data as value among the players, protecting the ability to

compete, through harmonized rules on fair access to and use of data. Also, it intends to increase legal certainty.<sup>1</sup>

Furthermore, some of the measures established on the draft of Data Act are: means to allow users of connected devices to gain access to data generated by them, means to rebalance negotiation power for SMEs by preventing abuse of contractual imbalances in data contracts, means for public sector bodies to access and use data held by the private sector that is necessary for exceptional circumstances, particularly in case of a public emergency, as well as, rules allowing customers to effectively switch between different cloud data-processing services providers and putting in place safeguards.<sup>2 3</sup>

## 2.2. SMEs

Primarily, SMEs are defined in EU by the Annex of Recommendation 2003/361/EC in Article 1 and 2. They are micro, small and medium-sized enterprises, which have as determining factors the staff headcount, annual turnover and/or annual balance sheet total. Medium-sized enterprises are with fewer than 250 persons, not exceeding EUR 50 million on turnover and EUR 43 million on balance sheet. Small-sized enterprises have fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million. For micro-sized enterprises it is less than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.<sup>4</sup>

Following this analysis of definition and other subsequent articles, like Article 3, it is possible to conclude that cooperation between SMEs that still fall under the requirements of Articles 1, 2 and 3 will keep exempting them. This is concluded from the combination of those articles and the text of Article 7 of draft Data Act.

## 3. Access Rights and their Scope of Application

Especially after the awareness gained regarding the capability of the devices that collect information via technologies such as internet of things (IoT) as well as produce their own information (machine generated data), various data that is gathered by smart devices

---

<sup>1</sup> 'What Impact Will the EU Data Act Have on the Digital Economy?' (*World Economic Forum*) <<https://www.weforum.org/agenda/2022/03/the-impact-of-the-eu-data-act-on-the-digital-economy/>> accessed 13 October 2022.

<sup>2</sup> 'Data Act: Measures for a Fair and Innovative Data Economy' (*European Commission*) <[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1113](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)> accessed 13 October 2022.

<sup>3</sup> 'Data Act | Shaping Europe's Digital Future' (*European Commission*) <<https://digital-strategy.ec.europa.eu/en/policies/data-act>> accessed 13 October 2022.

<sup>4</sup> 'Commission Recommendation of 6 May 2003 Concerning the Definition of Micro, Small and Medium-Sized Enterprises (Text with EEA Relevance) (Notified under Document Number C(2003) 1422)', vol 124 (2003) <<http://data.europa.eu/eli/reco/2003/361/oj/eng>> accessed 14 October 2022.

(IoT) are only used by the manufacturers who own the device. That is why, with this motivation, draft Data Act has been implemented in order to prevent the dominance and monopoly over the data produced by the users of these devices. It is aimed to increase the users' flexibility and access right over the machine data produced by the devices based on the preferences of the users and machine-learning capacities of the devices in question. One of the biggest aims of draft Data Act is to provide interoperability between the smart devices/applications; while also considering to establish better conditions for secondary market services also by improving the competing power of micro, small and medium sized enterprises as market players.

### **3.1. Types of Data subjected to Access Right**

For providing afore-mentioned results, draft Data Act, with Articles 3 and 4 under Chapter II titled as *“Business to Consumer and Business to Business Data Sharing”*, regulate access rights of both consumers and businesses to the machine generated personal or non-personal data upon the request of the user and provide data flow with the insight that data generation procedures have two-sided approach; manufacturer as well as the user. According to the articles in question, it is aimed that users of a product or related service in the Union, can access to the data generated by the use of that product or related service and that those users can use the data, including sharing them with third parties of their choice. That is why, upon the simple request of the data user as data subjects (that is granted via automatic execution measures), data holder is under obligation to provide access to the data to its users as well as to make the data available to third parties of the user’s choice. Even though the data that is generated by device and cannot be linked to the use of the device of the user in question is not subjected to this right; data that is gathered by the use of the product or related service including the data recorded intentionally by the user of the product/service constitutes a valid ground for the access right as it is introduced by Article 3, including Recitals 17 and 24.

### **3.2. Categorization of Machine-Generated Data and GDPR**

When considering the nature of the machine generated data and as it is illustrated by Communication from Commission to EU Parliament on *“Building a European Data Economy”* dated January 2017; *“Machine-generated data can be personal or non-personal in nature. Where machine generated data allows identification of a natural person, it qualifies as personal data and be subjected to GDPR.”* That is why, Data Act may also provide the data flow of personal data which needs to be practiced in accordance with the regulations and safeguards of GDPR. Similarly, while regulating the data flow between businesses or consumers, draft Data Act is actually referring to GDPR, while preserving the principles to process personal data. According to Recital 7 of the draft Data Act; *“No provision of this Regulation should be applied or interpreted in such*



*a way as to diminish or limit the right to the protection of personal data or the right to privacy and confidentiality of communication, in particular Regulation (EU) 2016/679 (GDPR)."* Therefore, data minimisation principle that foresees data controller to limit the processing and collection of the personal data that belonging the data subjects to what is directly relevant and necessary to accomplish a specified purposes well as the use of the data for only the specified purposes (Article 5 of GDPR);<sup>5</sup> and data protection by design and default especially when there are significant risks to fundamental rights of data subjects shall also be strictly sought by draft Data Act. It is also referred by Recital 8 of Data Act that all parties involved to data sharing as a result of the access rights are obliged to take the necessary up-to-date and proper technical and organisational measures including pseudonymisation and encryption to protect the rights of data subjects/users.

While transferring the data as it is requested by the user; also, appropriate user identification measures might be used by data holder for verifying the entitlement to access the data in question and in the cases of personal data transfer, it is also expected by data holder, who is Controller to ensure the request of the user to be conducted by the processor who is processing the personal data on behalf of the controller, as specified in Recital 27.

### **3.3. The Effects on SMEs Position**

The access right that is introduced under Chapter II of Data Act is not only for increasing the control of the users on the data gathered by the use of the product or related service; but also for increasing limited-digital capacities and skills of micro small and medium sized enterprises to collect, analyze and use the data and avoid limited interoperability because of the data dominance of bigger players in the same market. Under the current circumstances, due to the inefficient level of incentives of entering voluntary data sharing agreements between data holders and third parties; competitiveness as well as innovations that drives from high quality and interoperable data are not provided. That is why, thanks to the increased possibility to provide data flow between different players in the same market, more actors including micro, small and medium sized enterprises is expected to be encouraged to participate in data economy in EU since after such access to the data of the user has been provided, the user is entitled to use the data that is gathered by the product or service in question for any lawful purposes.<sup>6</sup> Moreover, not only the variety of the actors but also quality of the data is expected to be increased due to the incentives for manufacturers to provide investing in the high-quality data generation. As a result, after the aforementioned data dominance and the unequal competitive ability of market players are improved, more

---

<sup>5</sup> 'Data Minimization' (*European Data Protection Supervisor March 16, 2022*); <[https://edps.europa.eu/data-protection/data-protection/glossary/d\\_en](https://edps.europa.eu/data-protection/data-protection/glossary/d_en)>; accessed 6 October 2022.

<sup>6</sup> Data Act | Shaping Europe's Digital Future (n 3).

cost-efficient solutions will be provided to the users; especially with the participation of actors of all sizes, the after-sales services that can be provided for the aforementioned IoT devices will be developed more efficiently; and more concrete steps can be taken towards standardizing high-quality data.

#### 4. Handling Over Data to Third Parties

As it was previously mentioned, the Data Act is designed to make data sharing easier to third parties.<sup>7</sup> Its aim is to regulate the distribution of personal and non-personal data,<sup>8</sup> by decentralizing the right to access and use of such data among multiple stakeholders. The Data Act regulates data sharing with third parties, through these provisions: Article 5 “*Right to Share Data with Third Parties*”, Article 6 “*Obligations of Third Parties Receiving Data at The Request of the User*”, and Article 7 “*Scope of Business to Consumer and Business to Business Data Sharing Obligations, to Regulate the Sharing of Data with Third Parties*”.<sup>9</sup>

##### 4.1. Defining Third Parties, Users and Data Holders

The Data Act in Article 2 “*Definitions*” does not define third parties. However, Article 5 “*Right to share data with third parties*” outlines third parties, as those which acquire access to data from data holders, only at the request of the user.<sup>10</sup> After which request the data holder must share data of the same quality with the third party, without undue delay, and if applicable, in real time. As a result of this provision, not all parties can fall under the category of third parties. In general, this regulation establishes a rule that third parties are those which get access to data, after the request of the user. Based on this approach, third parties cannot be public bodies, Union institutions, agencies and bodies, which get access to data at their direct request toward data holders. The same conclusion about third parties can be confirmed with Recital 5, which defines third parties and Recital 24, that explains the bases for data holders to share personal and non-personal data with third parties. Moreover, Recital 29 describes that third parties can be enterprises, research or a non-profit organizations. A more explicit understanding of third parties is provided in Recital 31 where among others is mentioned that “*Data generated by the use of a product or related service should only be made available to a third party at the request of the user.*”

---

<sup>7</sup> Data Act | Shaping Europe’s Digital Future (n 3).

<sup>8</sup> Antonia Herfurth, ‘The European Data Act’ (Alliuris) <<https://www.alliuris.org/the-european-data-act/>> accessed 13 October 2022.

<sup>9</sup> ‘Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) (European Commission) <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0068&from=EN>> accessed 14 October 2022.

<sup>10</sup> Data Act (n 9).

Apart from this general rule for identifying third parties, the regulation provides specific rules for exempting parties from the status of third parties. This hint is provided in Article 5 (2), which states that platforms designated as gatekeepers by the upcoming Digital Market Act, cannot have the status of a third party.<sup>11</sup> Based on this exemption, gatekeepers cannot get access on data from data holders, regardless of a request from a data user. One can come to the same conclusion by reading Recital 36, which clarifies why gatekeepers cannot be beneficiaries of the Data Act. However, this exemption does not prevent gatekeepers from being classified as data holders. Therefore, these platforms are obliged to share data with other third parties, at the request of the user.

The users based on the Data Act, is defined in Article 2 “*Definitions*” both as natural and legal persons that either own, rent or lease a product or a service. Also, more information on the rights of uses can be found in Recital 28 of the Regulation. Therefore, the user and its rights are clearly illustrated in the Data Act. In conclusion a user can be a physical person, or an enterprise which is simply producing data by using the product or service provided by the data holder.

Data holders, are also defined in Article 2 of the Data Act. Based on this provision, a data holder is any legal or natural person that has the right or obligation to make available certain data. However, Article 7 “*Scope of Business to Consumer and Business to Business Data Sharing Obligations*”, clarifies that micro and small enterprises are exempt from the obligation to share data with third parties, even though they can have the status of a data holder as defined on the Data Act. The same can be concluded by reading Recital 36. However, Recital 37 only exempts micro and small enterprises from the obligation to share data, when this would be an overburden for such parties, if they hold the status of a manufacturer, or the designer of a product or related service. Therefore, micro and small enterprises are actually obliged to share data with third parties, if they are subcontractors, or when such enterprises are not the manufacturer of a product or the provider of the related service. Nevertheless, these clarifications are only mentioned in Recital 37, whilst Article 7 (1) generally exempts all micro and small enterprises from the obligation to provide data if they are in the shoes of a data holder. Article 7, only excludes micro and small enterprises from the obligation to share data when such enterprises have partner enterprises or are linked with other enterprises as defined in Article 3 of the Annex Recommendation 2003/361/EC. This means that Article 7 of the Data Act, obliges micro and small enterprises to share data with third parties, if they are in partnership or are linked with other enterprises. Hence, it may be unclear in what circumstances micro and small businesses are exempt from the requirement to exchange data with third parties, even if they hold the status of data holders, due to the discrepancy between Article 7 and Recital 37 of the Data Act.

---

<sup>11</sup> ‘The Digital Markets Act: ensuring fair and open digital markets’ (European Commission) <[https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en)> accessed 12 October 2022.

## 4.2. Third Party Responsibilities

This regulation was designed to create more opportunities for third parties, by giving rights to gain access and use data in order to drive innovation in the digital economy. Anyhow, in order to keep a balance of rights and obligations, the Data Act also defined the responsibilities of third parties by introducing Article 6.

In an overview, this article concludes that third parties can only process the data under the condition and for the purpose agreed with the user, which may be a data subject if the data is personal data. And generally, third parties are obliged to delete such data when processing is no longer necessary for the agreed purpose.

Alongside, Article 6 (2) of the Data Act provides an exhaustive list of behaviors from which third parties must refrain to engage. Some of the forbidden behaviors are there to protect the user, while others to protect the data holders, to ensure fair competition, and to disallow sharing of data with gatekeepers.

Furthermore, Recital 34, explains that third parties cannot engage in dark pattern behaviors, should adhere to the principle of data minimization, and should engage in behaviors that respect consumer rights. Recital 35 clarifies that third parties should refrain from profiling individuals, or even data holders, and should not use such data on creating products which are directly competitive with the original product of the data holder.

## 4.3 Relationship with Competition

The Regulation aims to create an environment which would help competition.<sup>12</sup> Its approach can be defined in two lanes: a) protecting information related to the economic situation, assets or production methods, that would undermine the position of third parties; and b) preventing third parties from using data to create a direct competitive product, with the original one manufactured or provided by the data holder.

Regarding the first part, Article 5 (5) prohibits data holders from using data to infer information on the economic situation, or know how of the third party that would undermine its commercial position. The data holder must be careful especially when it is in direct competition with the third party, as provided in Recital 29.

---

<sup>12</sup> 'The Data Act – Sharing is Caring. Or is it?' (GMW-BLOG) <  
<https://www.glademichelwirtz.com/en/blog/the-data-act-sharing-is-caring-or-is-it/>> accessed 14 October 2022.

Secondly Article 6 (2) (c) prohibits third parties to develop products that compete with the original products from which the data was provided in the first place from the data holder. The same prohibition is also explained in Recital 35.

However, the Data Act explicitly states that the user can share data, or can even ask the data holder to share data with a third party, even if the latter is a competing party of the data holder. This is explained thoroughly in Recital 28. Nonetheless the user, is only free to request the data holder to share data with third parties, if the data holder and the third party are in competition in the aftermarket service. Yet, there is no information in the Data Act, if the user can share data or ask from the data holder to share data with a third party, if this party is a direct competitor in the upstream market of the data holder.

### **4.3. IP Rights**

Data Act in general recognizes Intellectual Property rights, and in particular trade secret and sui generis database right when sharing data with third parties. The Data Act might obtain different approaches for different categories of IP rights and it still remains unclear how in particular trade secret will be protected under Data Act.

From the perspective of sui generis database protection; according to the draft Data Act; if the user requests access to the data which might be protected under the sui generis database right as well as its transfer to third parties; it is not possible for the Data Holder to object to this request unless it is provided that this right will be preserved. In particular, the Data Holder, to whom these requests are submitted, asserting its own conflicting interests; cannot avoid fulfilling this request when the necessary conditions are met. As it is regulated under Article 15 of Database Directive; investment in obtaining, verifying and presenting the data even though database itself cannot be subjected to copyright protection, in other words, not the creation of data but the product of another economic activity is protected (CJEU). With the help of Data Act; the intervention on the sui generis right is tried to be addressed since there is a problematic application of the sui generis right in the Internet of Things context. In order to eliminate the risk that data holders of databases obtained or generated by IoT and a related service claim the sui generis database right without qualifications; while aiming to hinder effective exercise of the right of users to access and use data and the right to share data with third parties, it is now clarified that the sui generis right does not apply to such databases as the requirements for protection would not be fulfilled. (Chapter 10, Article 35 & Recital 84)

On the other hand, for protection of trade secrets: based on Article 5 (8) data holders are obliged to share their trade secrets or know how to third parties, when: a) it is strictly necessary for fulfilling the purpose agreed between the user and third party; and b) if all the confidentiality measures are agreed upon data holders and third parties. This

might be interpreted as an obligation on the data holder, to share data classified as trade secrets (when linked with the User) with third parties at the request of the user. However, Article 8 (6), states that data holders are not obliged to disclose information to data recipients.<sup>13</sup> Because of these two contradicting articles, a confusion on the obligation of the data holder might arise, with regards to data holders' duty to share data classified as trade secrets.

In general, the implementation of the Data Act, is not supposed to affect intellectual property protection, including trade secrets. Because the same trade secret protection acquired by Directive (EU) 2016/943 is also recognized by the new proposal. However, in practice this might not be the case. Since this Regulation is not clear in defining whether there is an obligation of the data holder to share data classified as trade secrets, if it is strictly necessary and protection of confidentiality is preserved. Or does the Regulation, recognize the data holders right to refuse to a request to share data with a user, third party, even if both the above-mentioned conditions are met.

On the other hand, it is clear that the Data Act through Article 19 (2) and Recital 66, oblige data holders to disclose trade secrets to public sector bodies, if it is strictly necessary and under insurance of confidentiality. In conclusion, data holders must actually disclose information with public authorities when the above-mentioned conditions are met.

## 5. Deletion of Data with the Data Act

The draft proposal of the European Commission, the Data Act, aims to regulate sharing and using of data beyond data holders, to consumers, businesses and at exceptional need, to public bodies and Union institutions, agencies.<sup>14</sup> With the enforcement of this regulation, the data which was once held and used by one party "the data holder", now has the possibility to be reproduced and used by other parties "the data receivers". An aftereffect of data sharing will be the prolongation of data usage between multiple parties. Alongside this will affect the process of deletion of data. Sharing of data at different periods of time to new parties, will bring questions such as:

- Who is liable for data erasure after giving access to third parties;
- When will the data be considered "no longer necessary" in a chain of data shares;
- Uncertainty to the use, as to the fact when is the data in reality deleted.

---

<sup>13</sup> 'Why IP lawyers need to pay attention to the EU's draft Data Act' (*Bird&Bird*), <<https://www.twobirds.com/en/insights/2022/uk/why-ip-lawyers-need-to-pay-attention-to-the-eus-draft-data-act>> accessed 12 October 2022.

<sup>14</sup> Data Act | Shaping Europe's Digital Future (n 3).

## 5.1. Status quo

Currently, the deletion of data is only regulated for personal data, by Article 17, “*Right to Erasure*”, GDPR.<sup>15</sup> This provision clearly foresees the right of data subjects to request the erasure of personal data, and the obligation of the data controllers to erase that data without undue delay. This erasure should be done under one of the following reasons: if the data is no longer necessary, if the data subject withdraws consent, if the data subject objects the processing of data, and if data was unlawfully processed. Beyond this, Article 17 (2) of GDPR clearly states the obligation of the controller to inform other controllers for the erasure of such data, in cases when the data was shared or if it was made public. This provision of GDPR provides clear obligations on the original controller of data to take reasonable steps, including technical measures to erase the data, even if that data was shared to more parties. However, this regulation is strictly applicable to personal data.

## 5.2. Data Act and Its Effect on Deletion of Data

As aforementioned the current draft of Data Act regulates non-personal and personal data sharing. The deletion of these type of data is vaguely arranged through Article 6 (1), Obligations of third parties receiving data at the request of the user, Article 19 (1) (c) Obligations of public sector bodies and Union institutions, agencies and bodies, Recital 35 referring to the application of Article 17 of General Data Protection Regulation (GDPR) when personal data is involved, and Recital 65 concerning the deletion of data acquired at exceptional need by public bodies.<sup>16</sup>

The Data Act treats the deletion of data in three categories:

- Deletion of personal data shared with third parties;
- Deletion of non-personal data shared with third parties;
- Deletion of personal and non-personal data shared with public bodies.

The deletion of personal data shared with third parties clearly points to the application of Article 17 of GDPR through t Recital 35 of Data Act. This implies that personal data which is shared with third parties, at the request of the user “data subject”, should be deleted by the data holder “data controller”. This is the case when data is no longer required to be processed for the purpose agreed to by the user. This recital of the Data Act makes the data holder responsible for erasing data, and taking reasonable measures to inform other third parties to erase such data.

---

<sup>15</sup> ‘General Data Protection Regulation GDPR’ (*Intersoft Consulting*) < <https://gdpr-info.eu/>> accessed 16 October 2022.

<sup>16</sup> Data Act (n 9).

On the other hand, the situation is hazy when it comes to deletion of non-personal data shared with third parties. Data Act through Article 6 (1) explains that the third party shall delete the data when such data is no longer necessary for the agreed purpose of sharing of such data. This article leaves gaps on explaining if the third party is responsible itself for the deletion of data, or this should be done at the request of the user. This uncertainty is created due to the fact that the third party gets access to data by the data holder, only at the request of the user. It is also unclear if the first data holder has responsibility to inform third parties, for the deletion of data. And lastly there is no information as to which party does the principle of “no longer necessary” apply in the end.

Whilst, the deletion of data shared with public authorities is regulated mainly through Article 19 (1) (c) of the Data Act. This article makes the public body liable to destroy the data when they are no longer necessary, and to inform the data holder about the fact that the data was destroyed. The same explanations can be found on Recital 65.<sup>17</sup> These provisions, clarify that the responsibility for the deletion of data is on the public authority. Nonetheless, even in this clause, it is not quite clear when the data is no longer needed for the purpose for which it was supplied.

## **6. Contractual power of SMEs**

Not only from access rights perspective but also from unequal competing conditions perspective, the disadvantageous position of SMEs is regulated by draft Data Act. Even though there are cases that the draft of the Data Act does not include all enterprises, only micro and small, as they are in a disadvantage with medium-sized ones in relation to staff and finances; all of them, micro, small, and medium-sized are in a big disadvantage in market power, staff, finances, territory, also relevant in this case the bargaining position, in which big companies are stronger.

As it is explained so far, similarly the reasoning for underlying rules to rebalance this relation and avoid monopoly from big companies is to allow flexibility, increase innovation and guarantee competitiveness. The SMEs are good for this because they are always creating new products and services, investing in their adaptation to new technologies and regulations.

Generally, freedom of contract remains the main principle of contracts, however, whenever one party is in a stronger bargaining position there is a risk for imbalance in the negotiation of data agreements, as explained in Recital 51 and 52<sup>18</sup> of the draft Data Act. This situation may lead to ‘take-it-or-leave-it’ contractual terms, which the other

---

<sup>17</sup> Data Act (n 9).

<sup>18</sup> Ibid.



party has no choice other than accepting. Therefore, unfair contract terms regulating the access to and use of data or the liability and remedies for the breach or the termination of data related obligations should not be binding on micro, small or medium-sized enterprises when they have been unilaterally imposed on them.

## **7. Data Agreements**

### **7.1. Unfair Contractual Terms**

In this respect, Chapter IV, Article 13(1) of draft Data Act states that a contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations unilaterally imposed by an enterprise on SMEs shall not be binding if it is unfair. In the same article, it says in Article 13(2) that they will be unfair if it deviates from good practice, or contrary to good faith. Also, it establishes the absolute unfair terms in Article 13(3) (a)(b)(c) and the presumed ones in (4) (a)(b)(c)(d)(e).<sup>19</sup>

The unilateral aspect is defined in Article 13(5), as the ones imposed by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. In which also establishes that the contracting party that supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed.<sup>20</sup>

Relevant to highlight that Article 13(6) states that other terms may still be binding when severable from the unfair ones. In addition, Article 13(7) says that it does not apply to contractual terms defining the main subject matter of the contract or to contractual terms determining the price to be paid.<sup>21</sup>

Moreover, in the same way, on Recital 52 and 53<sup>22</sup>, reinforce about the contractual freedom for business relationships, in a way that not all terms should be subjected to the unfairness test, only the ones unilaterally imposed and related to making data available.

Consequently, this Regulation actually aims to rebalance negotiation power for SMEs by preventing abuse of contractual imbalances in data contracts, shielding them from unfair contractual terms imposed by a party with a significantly stronger bargaining position. Also, means that clauses in relation to data that do not pass this unfairness test will not be binding on SMEs.

---

<sup>19</sup> Ibid.

<sup>20</sup> Ibid.

<sup>21</sup> Ibid.

<sup>22</sup> Ibid.

Furthermore, looking from the practical implementation and implication of Data Act, some criticisms arise, also wondering about examples in real situations.

First, Article 13(2) arises a question concerning the interpretation of “nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing”, in a way that it will be expected a period of uncertainty until courts or other authorities establish interpretative guidance<sup>23</sup>.

Second, Article 13(5) brings a question regarding the burden of proof, it is reversed and for proof of a negative fact, which makes it challenging, because it is the need to prove that there was not an attempt to negotiate from the other party<sup>24</sup>.

Third, in relation to the unfair terms or deemed to be in Article 13(3) and (4) there are wondering of which would be examples to fit its descriptions. As Article 13(3) stipulate that a term is unfair if (a)exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence; (b)exclude the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations or the liability of the party that unilaterally imposed the term in case of breach of those obligations; or (c)give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract. As well as, Article 13(4) states that a term is presumed unfair if (a)inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations; (b)allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party; (c)prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner; (d)prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination thereof; or (e)enable the party that unilaterally imposed the term to terminate the contract with an unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for doing so.<sup>25</sup>

---

<sup>23</sup> Emre Bayamlıoğlu, ‘Chapters III and IV of the Data Act - B2B Data Sharing and Access.’ (*CITIP blog*, 30 June 2022) <<https://www.law.kuleuven.be/citip/blog/chapters-iii-and-iv-of-the-data-act-b2b-data-sharing-and-access/>> accessed 14 October 2022.

<sup>24</sup> Ibid.

<sup>25</sup> Data Act (n 9).

Some examples to simplify can be a clause stating that a company can unilaterally interpret the terms of the contract, clause stating a right to unilaterally vary the contract, clause stating a right to terminate without reasonable cause, clause to limit liability. It remains to be seen how it will affect the contracts in real situations and how courts will understand these agreements when there is a dispute.

## **7.2. Modal contractual terms**

Regarding data agreements and its terms to ensure fairness, Chapter IX, Article 34 of draft Data Act establish that the Commission shall develop and recommend non-binding model contractual terms on data access and use to assist parties in drafting and negotiating contracts with balanced contractual rights and obligations.<sup>26</sup> According to the aim of the legislation, these standard clauses will help SMEs negotiate fairer and balanced data contracts with companies enjoying a significantly stronger bargaining position.

## **8. Business to Government (B2G) Data Flow**

After facing a challenging global outbreak, Covid-19, now the ability of public entities to reach the data that is held by private entities is deemed as necessary by European Union. That is why, according to new regulations of the Data Act, Articles 14 to 22 and as it is explained under Recitals 56-65; in the events of exceptional need, the private entities will be obliged to make the data that they own to be accessible by public sector bodies including Union institutions, agencies or bodies upon their request.

### **8.1. Public Interest and Exceptional Need as a Concept: Public Emergencies and other Exceptional Cases**

First of all, determining which situations will constitute the public interest may be deemed necessary for the exercise of this right. According to Recital 56, situations that can trigger public interest and thus B2G (business to government) data flow, the exceptional need is referred and the concept exceptional need is examined in two categories; public emergencies and other exceptional cases. Public health emergencies such as a global viral outbreak, emergencies that originates from environmental disasters including climate change related disasters, large-scale/major problems, such as serious cybersecurity attacks from human intervention are considered as public emergency, therefore cause public interest (Recital 57). Exceptional need, on the other hand, may arise especially for taking preventive measures for public emergencies as well

---

<sup>26</sup> Ibid.

as measures for recovery from a public emergency, especially if especially there is strong evidence that the relevant public emergency will occur (Recital 58). However, Data Act did not consider both cases (public emergencies and other exceptional cases) as dependent on the principle of limited number (*numerus clausus*), on the contrary, it tried to diversify the situations by exemplifying. That is why, according to the same Recital, a public sector body will be able to use this right of access to data held by private entities upon request, if it encounters a time constraint for the efficient performance of any public duty/task in the law that concerns the public interest (such as official statistics).

## **8.2. Obligations of Private Sector Entities to Make the Data Available**

While regulating such access right of public sector bodies to private sector data; procedures to request the data as well as the prerequisites for the request to meet also introduced by Data Act. For providing efficient and functioning as well as proportionate framework for B2G data flows and access right in the cases of exceptional need; request shall be transparent and proportionate when considering their scope of content while also it is expected from public sector body to clearly and specifically state the intended purpose of use even though it is possible to provide a flexibility with the aim of providing full performance of the tasks in question in accordance with the public interest. Moreover, from the point of Data Act, it is also important to balance the interests as well as minimising the burden on the private entities while regulating such access right, with the aim of protecting the legitimate interests of private entities which the request has been made. For providing this, “once-only principle” has been introduced by Data Act and thanks to that, once a request has been made by one public sector body, it is not possible to claim another request for the same data in question. Moreover, for providing even higher level of transparency and to limit the access right of the public sector authorities, it has also been introduced by Recital 65 of Data Act that the data which is made available to public authorities can only be used in accordance with the stated purpose on the data access request, however, the data holder also can expressly agree for data in question to be used for also other purposes.

It is also important to mention that, once a request from the public sector body has been submitted to private entity as the data holder, the name of the entity and the request itself shall be made public without an undue delay for providing higher level of transparency during this process as well as justifying the reason and initiation behind the access request of the public sector entity. In addition, it is also possible for private entities whom the request has been submitted to ask for modification of the request as well as its cancellation, while illustrating a justified reason that leads private entity for this request, within 5 or 15 working days period when considering the nature of the submitted request as well as the exceptional need that embodies the request. Under those circumstances, based on the fact that the same data has been subjected to prior

request that originates from the same public emergency or other exceptional case, the private entity is entitled to reject to provide such access right to public entity.

### **8.3. Requests Regarding Personal Data**

While regulating such access right on behalf of the public sector bodies, Data Act has introduced a limitation regarding the accessibility of the personal data that is processed by private entities as data holders and it is regulated that personal data will not be subjected to such access request as long as it is deemed as strictly necessary by the public sector body that issues such a request. This strict necessity shall be demonstrated by the public sector body in the access request as well as purpose limitation measures for processing personal data in question and private sector entity as the data holder, if possible, shall anonymize the data or provide efficient level of effort for taking the possible technological measures before providing such access right to public sector bodies. Especially for providing appropriate level of protection to personal data, also in line with GDPR, necessary safeguards shall also be taken while making the data available.

### **8.4. Position of SMEs on B2G Data Flow**

After regulating such access right for providing business to government data flow in the cases of exceptional need; for avoiding an additional burden; draft Data Act has explicitly introduced an exemption on behalf of small and micro enterprises as defined under Article 2 of the Annex to Recommendation 2003/361/EC. That is why, even in the cases of public emergency, small and micro enterprises do not constitute a party for public sector bodies to request access right to the data that is held by them. However, medium sized enterprises may be subjected to access requests of the public sector bodies according to Article 14 (2) of draft Data Act. This regulation is also in favour of the SMEs while trying to increase their activity while not putting additional requirements for the organization. Moreover, it might be also understood that, one of the main aims of exceptional need to use the data via B2G data flow is actually to reach the data for taking the preventive or recovery measures or to fulfill a public duty/task as quickly and effectively as possible. That is why, since also small and micro sized entities are not eligible to process various forms of content and data; to introduce such access right of public sector bodies also on their data may not match with the reasoning of this regulation.

## **9. Switching Between Service Providers: Cloud and Edge Computing and Interoperability**

As it is clarified under Recital 71 of draft Data Act; *“Data processing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources.”* As a natural consequence of increasing free-flow of data, there will be an increased interest in data storage methods especially for cloud and edge computing methods. For this reason, equal competition conditions as well as competing power should also be provided among the actors providing storage services, in a way that allows actors of all sizes to store their own data. Similarly, for avoiding entry barriers resulting from contractual as well as technological conditions and to provide effective measures for switching between the data processing platforms such as edge and cloud computing services; the minimum level of standards via effective regulatory obligations have been introduced by draft Data Act.

It should be highlighted that; for providing the portability of the data especially meta-data, relatively easier conditions for termination of the existing conditions, ability to conclude multiple new contracts with various service providers, the technical measures for both transfer of the data as well as continuity to use the data in different platforms are tried to be provided by draft Data Act. According to Recital 79 of Data Act; reusable data structures and models (*in form of core vocabularies, ontologies, metadata application profile, reference data, taxonomies, code lists, authority tables, thesauri*) should also be part of the technical measures for semantic interoperability of the common European data spaces, application programming interfaces, and also cloud switching methodologies.

As further explained under Recitals 74 and 75 of draft Data Act; the efficient level of support and assistance shall be provided during switching period especially for avoiding additional categories of service solely based on the IT infrastructure and to some extent guarantee the functional equivalence between the platforms. In addition, to balance the competing power of the service providers especially during the switching period, standard contractual clauses are also advised to be developed by relevant bodies or expert groups.

Moreover, since one of the biggest treats about cloud computing services is unlawful access of the stored data by third parties; draft Data Act also introduced new obligations for cloud and edge service providers to take the necessary preventive measures (*such as encryption, cybersecurity certifications for verified adherence as well as internal precautions such as modification of corporate policies*) for avoiding undesirable access to the systems where the non-personal data is stored (Recital 78).

According to the *“Study on the Economic Detriment to Small and Medium-Sized Enterprises Arising from Unfair and Unbalanced Cloud Computing Contracts”* published by European Commission on November 2019: %64 of 503 SMEs declared that they have signed the standard contract terms and conditions of cloud service providers (p.5) and they have faced problems such as unsatisfactory availability or discontinuity of the

service (26%), low speed of the service (22%), and forced updates (13%) (p. 6) and the result showed that the contract-related cloud computing problems encountered harmed enterprises in terms of reputational damage and/or loss of clients, but these effects did not result in very significant changes in financial variables (i.e. in losses of turnover or profits (p. 10)).<sup>27</sup> That is why, it can be concluded that, the initiation of draft Data Act to introduce better conditions also for cloud and edge services including PaaS and SaaS solutions, is aiming to enhance the performance of the services of SMEs while improving their activities in the market which will end up with increased levels of customer satisfaction with uninterrupted service.

## 10. Practical Effects of Draft Data Act

Given the practical importance of the Data Act for SMEs, access rights shall need to be examined first. First of all, as explained in detail so far; at the request of the user, the sharing of all kinds of data produced by the device as a result of the use of the relevant device with third parties, including SMEs, is one of the most interesting regulations brought by draft Data Act. Although the free flow of "machine generated data" produced by the device is intended within the scope of this regulation; it does not seem possible to actualize the aforementioned data transfer completely without the involvement of personal data. In this case, although it is called non-personal data by the data holder; as a result of the possibility that the person/user may become identifiable during the transfer process, it can be concluded that each transfer shall be categorized as a kind of personal data transfer. In summary, although the data transferred by the data holder to third parties at the request of the user is non-personal data; it may be deemed as necessary to meet the conditions stipulated by the GDPR for personal data transfers.

In addition, no regulation is foreseen by the Data Act on the responsibility of the Controller as Data Holder stipulated by the GDPR. Although it is emphasized by draft Data Act that GDPR regulations will be protected, the liability regime of Data Holder/Controller is left unanswered especially in cases of a cyber-security vulnerabilities related to non-personal or personal machine generated data that is transferred to third parties upon the request of the user, or if there is a processing situation contrary to GDPR. There is no clear regulation as to whether the data holder, who is a controller, will be liable for the subsequent transfers of the third party to whom the data is transferred as a result of the request of the user.

---

<sup>27</sup> 'Study on the Economic Detriment to Small and Medium-Sized Enterprises Arising from Unfair and Unbalanced Cloud Computing Contracts' (European Commission) <[https://ec.europa.eu/info/publications/study-economic-detriment-small-and-medium-sized-enterprises-arising-unfair-and-unbalanced-cloud-computing-contracts\\_en](https://ec.europa.eu/info/publications/study-economic-detriment-small-and-medium-sized-enterprises-arising-unfair-and-unbalanced-cloud-computing-contracts_en)> accessed 12 October 2022.

Moreover, the Data Act is vague in identifying third parties. And as such, this definition is vital to implement this act, in order to share data for promoting innovative competition. Most crucially, it remains to be seen how the first product generating data will be protected from same emerging competitive products by third parties. Since in the end it will not be easy to make a clear differentiation, between a completely new innovative product from one that is a buy product of the first product that generated data.

Generally speaking, the Data Act's implementation is not anticipated to have an impact on the protection of intellectual property rights, including trade secrets. However, the Data Act creates ambiguity on understanding the obligations of data holders when requested by users to share data classified in trade secrets. Therefore, it will be fascinating to see how the Data Act impacts the disclosure of trade secrets to third parties.

Additionally, by sharing both personal and non-personal data between multiple parties, the Data Act creates uncertainty as to which party is responsible for insuring the deletion of the shared data. It is unclear whether this is the responsibility of the data holder, the third party or the user. In practice if the user requested the deletion of data from a data holder, which beforehand was also shared with a third party, is the data holder responsible to inform the third party about the erasure of such data. Or in this case does the responsibility falls under the user itself?

Moreover, by sharing data to third parties, the retention of data will be prolonged. As a consequence, the time for deleting data will be generally postponed. This due to the fact that when data becomes "no longer necessary" for one data holder, it might still be needed for the purposes of processing of such data by a third party.

It is believed that the afore-mentioned situation will also increase the uncertainty of the user to know when in reality the data is completely erased. Because, if one party deleted the data, the user will never know for certain if the same data was deleted by other third parties or public bodies.

As demonstrated before, this draft Act aims for legal certainty and fairness. However, in practice, the contractual clauses side of this Act will bring some questions in relation to interpretation. This is due to the fact that "good practice" is not easily defined, also it is not straightforward how to prove a negative fact when the burden of proof is reverse. For these situations and the lack of real practice contract clauses when assessing unfair terms will be likely to need some clarification through minor changes in the draft, or even if in force analyses by the courts. Although, a great result that can come is that the standard clauses that will be recommended will be helpful when defining in disputes the interpretation or assessment of unfair contractual terms, as the European Commission will set the goal in the suggested modal terms.

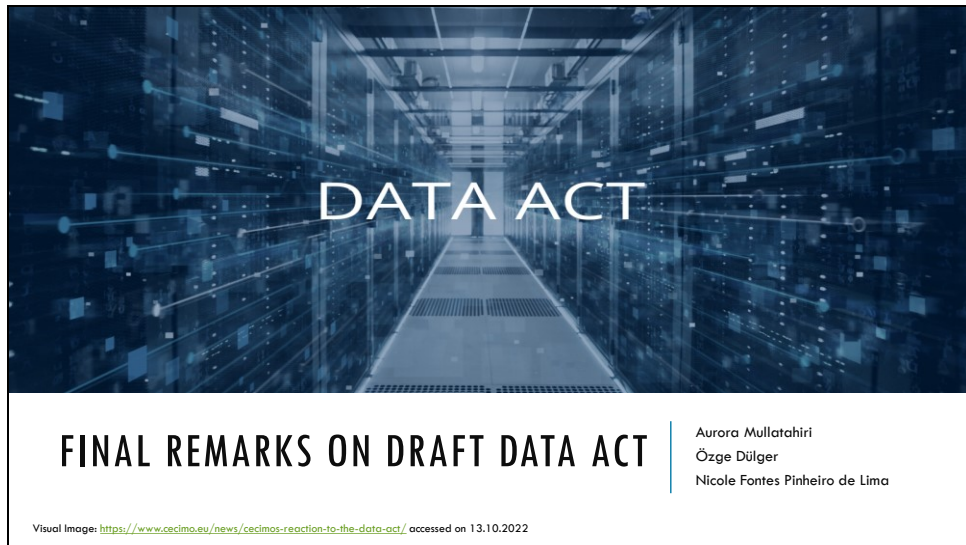


## 11. Final Remarks

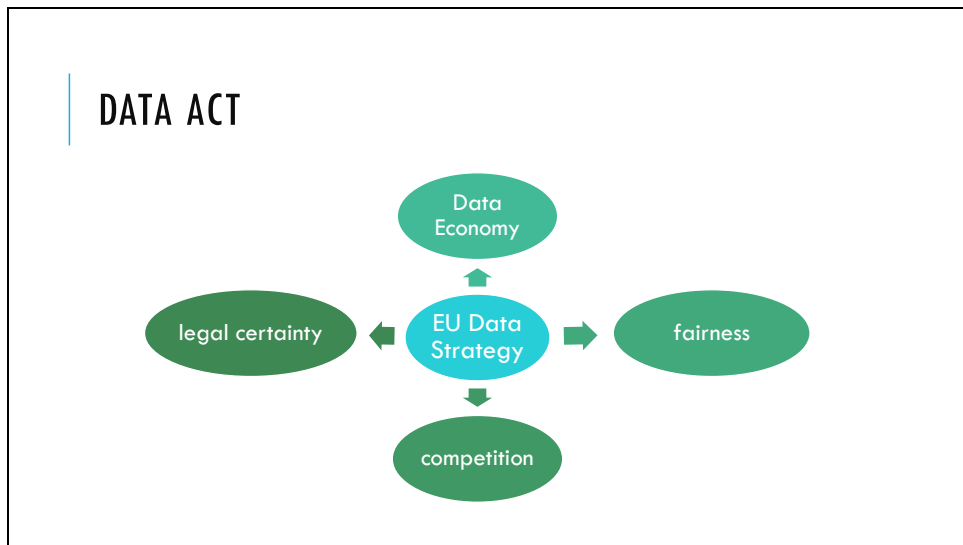
Data Act primarily aims to introduce higher standards to the European Data Economy, with more freedom, standardization and more actors in the market. In many respects, although it will eliminate the inequalities in the market for users' access to data as well as for SMEs to compete; It is also obvious that the draft Data Act remains silent and has provisions that may lead to uncertainties in implementation such as non-personal data flow including flows to third countries and liabilities of the Data Holders from further processing of the data.

Lastly, the Data Act will help third parties in receiving data, as a valuable asset to initiate innovation, and it will improve imbalances of the position of SMEs and gatekeepers in the digital market. However, this regulation will also increase data retention, it will impact the disclosure of trade secrets, and it will raise new questions for competition law.

+ + +



1



2

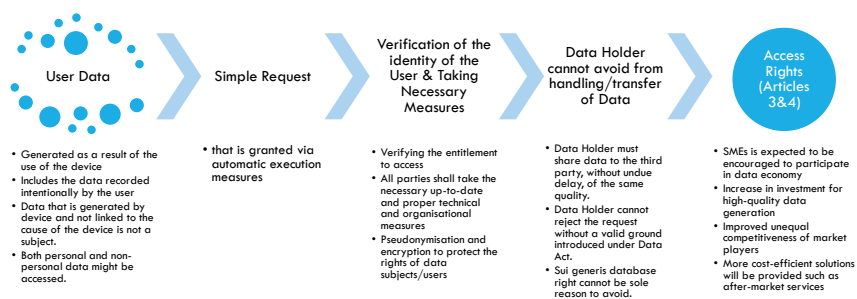
## SMES

Enterprise size	staff headcount	annual turnover	annual balance sheet
medium	250	EUR 50 million	EUR 43 million
small	50	EUR 10 million	EUR 10 million
micro	10	EUR 2 million	EUR 2 million

- What about cooperation between SMEs ?

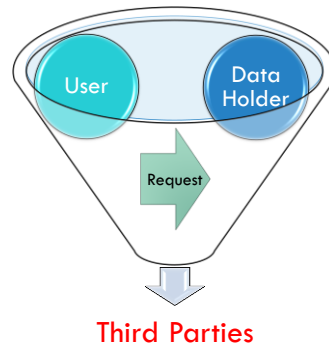
3

## 1. ACCESS RIGHTS



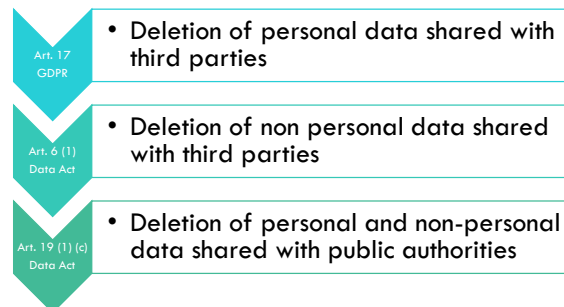
4

## 2. HANDLING OVER DATA TO THIRD PARTIES



5

## 3. DELETION OF DATA WITH THE DATA ACT



6

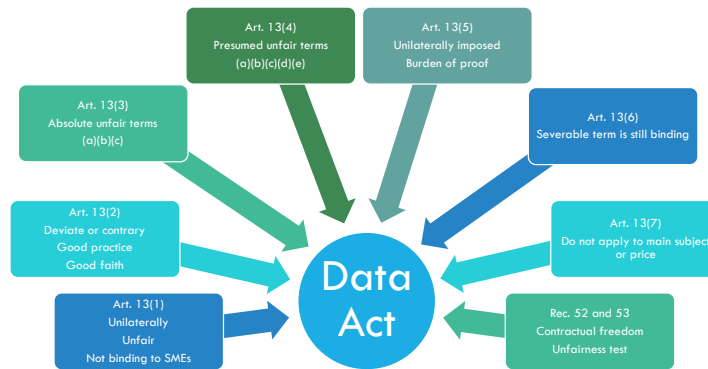
## 4. CONTRACTUAL POWER OF SMES



- Recital 51 and 52 of Data Act draft

7

## 5. DATA AGREEMENTS



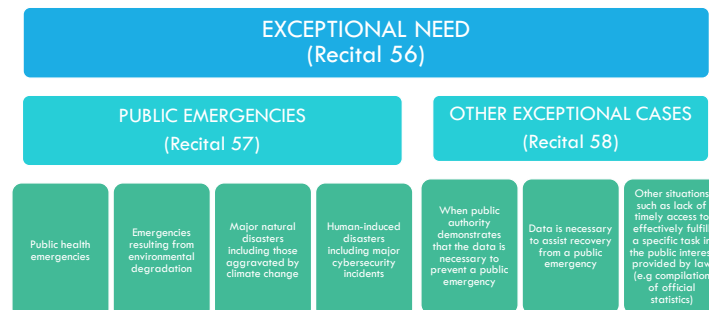
8

## 5. DATA AGREEMENTS




9

## 6. BUSINESS TO GOVERNMENT (B2G) DATA FLOW



10

## 6. BUSINESS TO GOVERNMENT (B2G) DATA FLOW



**EFFICIENT, WELL-FUNCTIONING & PROPORTIONATE B2G DATA FLOW**

- In case of an event that causes exceptional need

  - public emergencies
  - other exceptional cases
- Accessing the data that is held by private data holders (except micro and small enterprises)

  - For avoiding the additional burden on SMEs
  - If it is personal data, GDPR principles & safeguards are protected; if not strictly necessary it cannot be requested; if shared: technological measures such as anonymization etc.
- Data holders are obliged to provide access of to public sector bodies or to Union institutions, agencies or bodies upon their request.


  - request shall be transparent and proportionate
  - it is expected from public sector body to clearly and specifically state the intended purpose of use
  - "once-only principle" (not possible to claim another request for the same data)
- Once submitted, the name of the entity and the request itself shall be made public

  - higher level of transparency
  - without an undue delay
- Private entity can ask for modification or cancellation of the Request

  - based on a justified ground

11

## 7. SWITCHING BETWEEN SERVICE PROVIDERS



**Switching Between Service Providers: Cloud and Edge Computing and Interoperability**

- On-demand, broad remote access to a scalable & elastic pool of shareable and distributed computing resources*

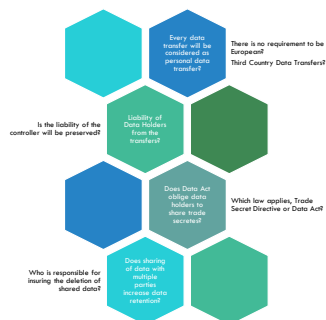
  - \* relatively easier conditions (for termination etc.),
  - \* ability to conclude multiple new contracts with various service providers,
  - \* the technical measures for both transfer and continuity to use the data in different platforms (reusable data structures and models)
- the efficient level of support and assistance shall be provided during switching period

  - guarantee the functional equivalence between the platforms
- new obligations for cloud and edge service providers to take the necessary preventive measures against unlawful access of third parties
- Aim is to enhance the performance of the services of SMEs

  - via improving their activities in the market e.g. customer satisfaction with uninterrupted service.

12

## POSSIBLE PRACTICAL EFFECTS AND FINAL REMARKS OF DRAFT DATA ACT



13

## QUIZ QUESTIONS

Q1: After the draft Data Act entered into force; can you (as the user of Philips Smart Bulbs and Xiaomi Smart Plugs) ask for Bestserviceever Startup to repair the unfunctionalities of those products?

Q2: Can a user request the data holder to share both personal and non-personal data to a third party, by the Data Act?

Q3: When unilaterally imposed by a party, is a clause limiting liability of a company for future situation of gross negligence binding?

14



## LAST PERSONAL QUESTION:

"When considering the explanations made so far, do you think draft Data Act will enter into force without major changes?"



YES



NO

15

## THANK YOU FOR YOUR ATTENTION!

ANY QUESTIONS?



16



## II.

---

# Artificial Intelligence

# Artificial Intelligence Risk Management

*Xiao YU, J.M. (China), Licensed Lawyer (China)*  
*Boğaçhan Emre Uysal, LL.B. (Turkey)*

*October 2022*

## 1. Introduction

Artificial intelligence (AI) has recently incorporated itself into our daily lives in ways that we might not even be aware of. It has spread so widely that many people are still oblivious of its effects and how much we depend on it. Our daily activities are mostly driven by AI technology from dawn to night.

There are some myths about AI to be corrected. First, the common worry about AI is that it would become conscious and evil one day. But what we really should worry about is that AI will turn competent with goals misaligned with us. Secondly, the image of AI usually is a robot, the true concern is the bodiless internet connection. They are misaligned intelligence. Last but not least, people are so afraid of the power of AI and believe it will conquer human race just in a few years. The truth is this technology still has a long way to develop.

The main dangers associated with AI are those that could hurt businesses, customers, or have a negative impact on society as a whole. These possible dangers could come from a variety of sources, including the data used to train the AI system, the AI system itself, how the AI system is utilized, and the AI system's general administration. These risks could also come from sources other than the data used to train the AI system.

## 2. AI Risk in the Financial Services Industry:

It's crucial to remember that the applicability and relevance of the risks rely on each organization's risk appetite, risk profile, and current controls. It is up to each company to decide if its current controls are enough.

### 2.1. Bias

Skewed AI systems may increase the likelihood of discrimination or unduly biased results. Data ethics, fairness, and the potential for unfairly skewed outcomes from the usage of AI, for instance, are still developing topics. However, it is clear that there is a chance that, depending on the use case, AI systems could produce unfairly biased results for people and/or organizations. Additionally, AI-driven unfairly biased outcomes may have concerns for privacy compliance, pose a risk for regulation, litigation, and reputation, have an influence on operations, and cause customer churn.

## **2.2. Limitations in Learning**

In contrast to humans, AI systems are deficient in context and judgment for many of the situations in which they are used. An AI/ML system's effectiveness is typically dependent on the data used to train it and the many scenarios that were taken into account. Most of the time, it is not possible to train the AI system on every scenario and piece of information. Lack of context, poor judgment, and general learning deficiencies may have a significant impact on risk-based appraisals and debates on strategic deployment.

## **2.3. Reliability of the Data**

Poor data quality is a problem for all systems, not only AI/ML systems, as it may limit the system's capacity to learn and may even have an adverse effect on how it makes future inferences and judgments. Incomplete data, inaccurate or inappropriate data, old data, or data used inappropriately are all examples of poor data quality. These flaws could lead to predictions that turn out to be inaccurate or bad, or they might prevent the desired goals from being met.

## **3. AI Risk in EU AI Act**

With the proposed AI Act, Europe may be confident in what AI has to offer. While the majority of artificial intelligence (AI) systems are safe and can help with many social problems, there are some AI systems that can cause hazards which need to be addressed in order to prevent unfavorable results.

The Regulatory Framework defines 4 levels of risk in AI: Unacceptable risk; High risk; Limited risk; Minimal or no risk. All AI systems considered a clear threat to the safety, livelihoods and rights of the people fall into the scope of unacceptable risk AI, which will be banned, from social scoring by governments to toys using voice assistance that encourages dangerous behavior. Limited risk refers to AI systems with specific transparency obligations. When using AI systems such as chatbots, users should be aware that they are interacting with a machine so they can take an informed decision to continue or step back. The proposal allows the free use of minimal-risk AI. This includes applications such as AI-enabled video games or spam filters. The vast majority of AI systems currently used in the EU fall into this category.

The most important is the high-risk AI system. They are particularly regulated in article 6 and 7 in the Act. They conclude:

- critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;
- educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- safety components of products (e.g. AI application in robot-assisted surgery);
- employment, management of workers and access to self-employment (e.g. CV-sorting software for recruitment procedures);
- essential private and public services (e.g. credit scoring systems denying citizens opportunity to obtain a loan);
- law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);

High-risk AI systems will be subject to strict obligations before they can be put on the market:

- adequate risk assessment and mitigation systems;
- high quality of the datasets feeding the system to minimize risks and discriminatory outcomes;
- logging of activity to ensure traceability of results;
- detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance;
- clear and adequate information to the user;
- appropriate human oversight measures to minimize risk;
- high level of robustness, security and accuracy.

Users assure human control and monitoring once an AI system is put on the market, while suppliers have a post-market monitoring structure in place. Authorities are in charge of market surveillance. Serious events and malfunctions will be reported by both providers and users.

#### **4. Other Factors in AI Risk Management**

AI risk management could help organizations learn, govern, monitor, and mature AI adoption. Be aware that determining potential AI risks is essential to creating a framework for operational risk and control. A gap analysis versus the currently in place controls might then be implemented if possible risks have been identified. This calls for an organized strategy, careful planning, and engagement from multiple control owners depending on the control library of the organization. The gap analysis' findings should then inspire the development of potential new or improved controls to reduce the identified potential AI/ML hazards. A variety of additional considerations, some of which we list below, should be made into AI risk management.

#### **4.1. Managing Third-Party Risks**

In order to scale, enhance computational capacity, and gain access to vendors who are a part of the larger fintech ecosystem, the use of AI deployment may entail third-party applications and/or data. Therefore, businesses might need to improve their third-party risk management (TPRM) skills. These advances could put to the test a number of current practices, including TPRM transparency regarding model interpretability, information security concerns for cloud based service providers, and more general worries about third parties' reliance on technology. Depending on the use case, companies may think about incorporating language in contracts for third parties that address the AI system's testing methodology, the understandability of the findings it generates, and/or any potential intellectual property rights that may come from system use.

#### **4.2. Three Defense Lines**

The three-lines-of-defense concept is used by the majority of financial institutions. It divides assurance from other risk oversight and independent challenge groups (the Second Line) and front line groups, who are typically responsible for business risks (the First Line) (the Third Line). AI governance frameworks should make sure that the criteria for supervision, challenge, and assurance are addressed during the development and application of AI systems. The second and third lines of defense should also make sure they have enough subject-matter expertise to successfully challenge the first line in analyzing the planned usage and deployment of the AI systems because both the possible threats and legislation linked to AI are evolving.

### **5. AI Risk in the future**

Now there have been several warnings about how artificial intelligence (AI) technology could change the workforce, particularly for tasks that are simple to automate. The truth is that in the near future, artificial intelligence will be able to perform the administrative duties that take up a large portion of managers' time by making it faster, better, and cheaper. Despite the fact that AI is not currently recognized by business law as a director, there are examples of robot directors like Vital who have succeeded in securing a seat in the corporate boardroom. AI is currently poised to play a significant role in corporate governance. There are numerous legal discussions that arise when AI is used in corporate decision-making. The first relates to AI's selection as a board member. Even though AI doesn't have a personality, the process of electing an AI to the board has already begun. The second conversation focuses on the potential effects of outsourcing corporate decision-making to AI. The third topic of discussion is about making judgments

based on the findings of AI's data analysis. Although the practice of appointing AI as board members is still in its infancy, it is currently increasingly usual in business to delegate decision-making to AI or to use AI to aid in decision-making. AI will ultimately prove to be cheaper, more efficient, and potentially more impartial in its actions than human beings. Thus, in the future, more unexpected risks related to AI will appear, such as is it possible to appoint an algorithm in the management board? What would be the risk behind them? Will the corporation law be capable to adapt to the AI Age? More questions await to explore.



## Q&A Section

### 1. What is the situation of AI Regulation in other jurisdictions?

#### 1.1. USA

In the USA, Joe Biden recently accepted “Blueprint for an AI Bill of Rights” which sets out some principles on AI algorithms. Which are:

- Safe and Effective Systems
- Algorithmic Discrimination Protections
- Data Privacy
- Notice and Explanation
- Human Alternatives, Consideration, Fallback

According to these principles people should be protected from unsafe or ineffective systems, should not face discrimination by algorithms and systems should be used and designed in an equitable way, should be protected from abusive data practices via built-in protections and should have agency over how data about them is used, should know that an automated system is being used and understand how and why it contributes to outcomes that impact them. Finally, people should be able to opt-out, where appropriate, and have access to a person who can quickly consider and remedy problems they encounter.<sup>28</sup>

According to the text, this framework applies to automated systems that have the potential to meaningfully impact the American public’s rights, opportunities, or access to critical resources or services and this framework describes protections that should be applied with respect to all automated systems that have the potential to meaningfully impact individuals’ or communities’ exercise of civil rights, civil liberties, and privacy, equal opportunities, access to critical resources or services.

Also, the U.S. Congress enacted National **AI Initiative Act** in January 2021 which aims to create new offices and task forces to aim to implement a national AI strategy.

#### 1.2. China

---

<sup>28</sup> White House, “Blueprint for an AI Bill of Rights”, [Blueprint for an AI Bill of Rights | The White House](#), Accessed on 14.10.2022

In China in March 2022 a regulation about the use of algorithms in online recommendation systems is accepted. According to this regulation, such services should be:

- Moral
- Ethical
- Accountable
- Transparent
- Disseminate Positive Energy

This regulation also mandates companies:

- To give users the option to opt out of being targeted.
- To notify users when an AI algorithm plays a role in which information will be shown.
- Prohibiting algorithms that use personal data to offer different prices to different consumers.

## **2. What are the main objectives of the AI Act in EU?**

The main objectives of the AI Act are:<sup>29</sup>

- Ensure that the AI system is safe and respects the EU Law and EU fundamental rights and Union values.
- Ensure legal certainty to facilitate investment and innovation in AI.
- Improve governance and effective enforcement of the law on fundamental rights and safety requirements regarding AI systems.
- Ease the development of single market for AI and prevent market fragmentation.

## **3. Who will be affected by the AI Act?**

First of all, people living inside the EU territory will be naturally affected by this AI Act. Secondly, the businesses that are located in the EU will be affected. But the action zone of the Act is not limited to the EU territories also it will have extraterritorial reach individuals or companies located within the European Union, placing an AI system on the market in the European Union, or using an AI system within the European Union

---

<sup>29</sup> Mauritz Kop, "EU Artificial Intelligence Act: The European Approach to AI", [2021-09-28-EU-Artificial-Intelligence-Act-The-European-Approach-to-AI.pdf \(stanford.edu\)](#), Accessed on 14.10.2022

would also be subject to the regulation.<sup>30</sup> Furthermore, EU governments will use the latest technology for border control to monitor third-country citizens, predominantly people on the move.<sup>31</sup>

EU expects an outcome from this Act like in the GDPR, which a lot of countries follow with small changes or like in copy-paste formats.

#### 4. Which fines are waiting for AI Act breachers?

There are 3 levels of fines in the draft of the AI Act:

- For use of prohibited systems and the violation of the data-governance provisions when using high-risk systems, the fines could climb up to €30 Million or 6 percent of global revenue which is even higher than envisioned in GDPR.
- All other violations fines are up to €20 Million or 4 percent of global revenue.
- Finally, for providing incorrect or misleading information to authorities will be fined a maximum of €10 Million or 2 percent of global revenue.<sup>32</sup>

#### 5. What is the expected most critical legal problem for the AI Act?

Alongside the hardness of regulating a new field which is not regulated before there are also some legal issues are waiting for AI Act. Some of the regulations which are in force now in or will be in force soon are already regulating AI in different senses and this could lead to a legal problem for precedence in EU. These regulations are:

- GDPR
- Digital Services Act
- EU Competition Law
- EU Rules on Electrical Devices

GDPR has a very broad definition for personal data, which causes GDPR to regulate AI providers while the new EU Digital Services Act has provisions on “algorithmic transparency” which covers AI. There are EU Rules on Electrical Devices and rules for the

---

<sup>30</sup> Misha Benjamin, [Kevin Buehler](#), Rachel Dooley, Peter Zipparo, “Proposed EU rules are just one more step toward global AI regulation. Here’s how smart organizations are preparing for compliance—and managing AI risk”. [What the draft European Union AI regulations mean for business | McKinsey](#), Accessed on 14.10.2022

<sup>31</sup> Nikolett Aszodi, Angela Müller, “A guide to the AI Act, the EU’s upcoming AI rulebook you should watch out for, [A guide to the AI Act, the EU’s upcoming AI rulebook you should watch out for - AlgorithmWatch](#), , Accessed on 14.10.2022

<sup>32</sup> Misha Benjamin, [Kevin Buehler](#), Rachel Dooley, Peter Zipparo (n-3)

financial and healthcare sectors that cover AI.<sup>33</sup> It is certain that there will be clashing provisions with EU Competition Law also.

The question of which law takes precedence is, at present, seen as the most important legal question.

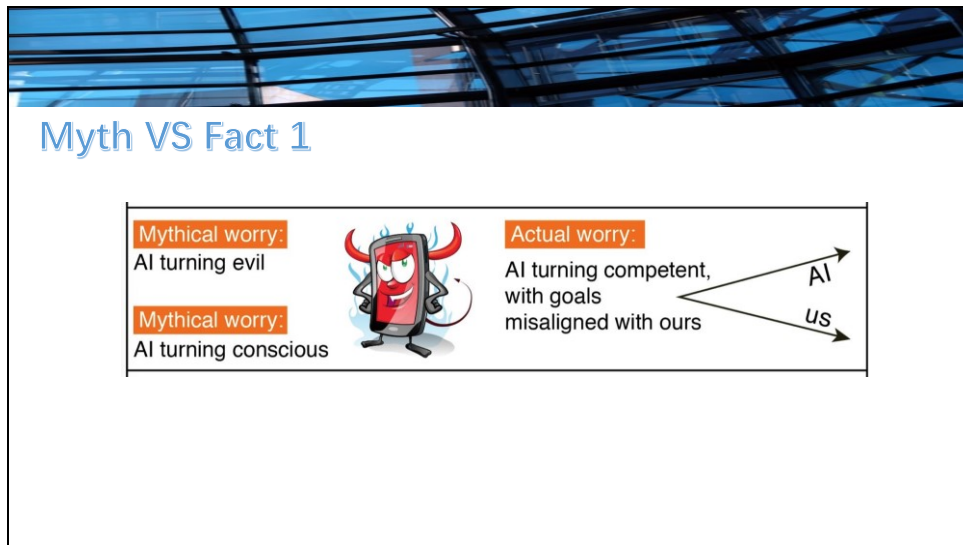
+ + +

---

<sup>33</sup> Axel Spies, "Germany and the EU Artificial Intelligence Act", [Germany and the EU Artificial Intelligence Act – AICGS](#), Accessed on 14.10.2022

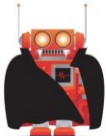


1





2

### Myth VS Fact 2

<b>Myth:</b> Robots are the main concern		<b>Fact:</b> Misaligned intelligence is the main concern: it needs no body, only an internet connection	<pre>0 0 1 0 1 1 1 0 0 1 0 1 1 1 1 1 1 1 0 0 0 0 0 0 1 0 0 1 1 1 1 0 0 0 1 0 0 1 1 0 0 1 0 1 1 0 0 0 0 1 1 0 0 0 0 1 1 1 1 1 0 0 1 1 0 0 0 0 1 0 1 0</pre>
---	---	--	--



3

### Myth VS Fact 3

<b>Myth:</b> AI can't control humans		<b>Fact:</b> Intelligence enables control: we control tigers by being smarter	
---	---	--	---

4

### Myth VS Fact 4

<b>Myth:</b> Machines can't have goals		<b>Fact:</b> A heat-seeking missile has a goal	
---	---	---	--

5

### Myth VS Fact 5

<b>Mythical worry:</b> Superintelligence is just years away	<b>PANIC!</b>	<b>Actual worry:</b> It's at least decades away, but it may take that long to make it safe	<b>PLAN AHEAD!</b>
--	---------------	---	--------------------

6



7

## AI REGULATIONS IN DIFFERENT JURISDICTIONS



8











## CHINA

IN MARCH, 2022 CHINA PASSED A REGULATION ABOUT THE USE OF ALGORITHMS IN ONLINE RECOMMENDATIONS SYSTEMS


9



### REQUIRING THAT SUCH SERVICES SHOULD BE:

-  MORAL
-  ETHICAL
-  ACCOUNTABLE
-  TRANSPARENT
-  DISSEMINATE POSITIVE ENERGY

10



THE REGULATION ALSO MANDATES COMPANIES:

- GIVE THE OPTION TO USERS TO OPT-OUT OF BEING TARGETED
- TO NOTIFY USERS WHEN AN AI ALGORITHM PLAYS A ROLE IN WHICH INFORMATION WILL BE SHOWN TO USERS
- PROHIBITING ALGORITHMS THAT USE PERSONAL DATA TO OFFER DIFFERENT PRICES TO DIFFERENT CONSUMERS


11



USA

- THERE IS A FRAGMENTED APPROACH IN DIFFERENT STATES. HOWEVER, U.S. CONGRESS ENACTED NATIONAL AI INITIATIVE ACT IN JANUARY 2021.
- THE ACT CREATED NEW OFFICES AND TASK FORCES TO AIM TO IMPLEMENT A NATIONAL AI STRATEGY.


12



**Colorado - CO S.B. 113**

- CREATES A TASK FORCE FOR CONSIDERATION OF FACIAL RECOGNITION SERVICES, WHICH IS DIRECTED, AMONG OTHER ISSUES, TO RECOMMEND WHETHER THE SCOPE OF THE TASK FORCE SHOULD BE EXPANDED TO INCLUDE CONSIDERATION OF ARTIFICIAL INTELLIGENCE.


13



**Illinois – IL H.B. 53**

- AMENDS THE ARTIFICIAL INTELLIGENCE VIDEO INTERVIEW ACT, PROVIDES THAT EMPLOYERS THAT RELY SOLELY UPON ARTIFICIAL INTELLIGENCE TO DETERMINE WHETHER AN APPLICANT WILL QUALIFY FOR AN IN-PERSON INTERVIEW MUST GATHER AND REPORT CERTAIN DEMOGRAPHIC INFORMATION TO THE DEPARTMENT OF COMMERCE AND ECONOMIC OPPORTUNITY, REQUIRES THE DEPARTMENT TO ANALYZE THE DATA AND REPORT TO THE GOVERNOR AND GENERAL ASSEMBLY WHETHER THE DATA DISCLOSES A RACIAL BIAS IN THE USE OF ARTIFICIAL INTELLIGENCE.


14



**Vermont - VT H.B. 410**

- PROPOSES TO CREATE THE ARTIFICIAL INTELLIGENCE COMMISSION TO SUPPORT THE ETHICAL USE AND DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN THE STATE, RELATES TO THE USE AND OVERSIGHT OF ARTIFICIAL INTELLIGENCE IN STATE GOVERNMENT.


15



**New Jersey – NJ S.B. 2723**

- CONCERNS THE MODERNIZATION OF STATE GOVERNMENT WEBSITES; RELATES TO 21ST CENTURY INTEGRATED DIGITAL EXPERIENCE ACT; ADDS DEFINITION; EVALUATES ON AN ANNUAL BASIS THE FEASIBILITY OF USING ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, AND COMMERCIAL CLOUD COMPUTING SERVICES, AS WELL AS OTHER EMERGING TECHNOLOGIES, BY STATE AGENCIES TO PROVIDE PUBLIC SERVICES AND THE DEVELOPMENT OF DATA ANALYTICS CAPABILITIES.

16



## Washington- WA S.B. 5092

- MAKES 2021-2023 FISCAL BIENNIUM OPERATING APPROPRIATIONS, INCLUDING APPROPRIATIONS SOLELY FOR THE OFFICE OF THE CHIEF INFORMATION OFFICER WHO MUST CONVENE A WORK GROUP TO EXAMINE HOW AUTOMATED DECISION MAKING SYSTEMS CAN BEST BE REVIEWED BEFORE ADOPTION AND WHILE IN OPERATION AND BE PERIODICALLY AUDITED TO ENSURE THAT SUCH SYSTEMS ARE FAIR, TRANSPARENT, ACCOUNTABLE AND DO NOT IMPROPERLY ADVANTAGE OR DISADVANTAGE WASHINGTON RESIDENTS.

17

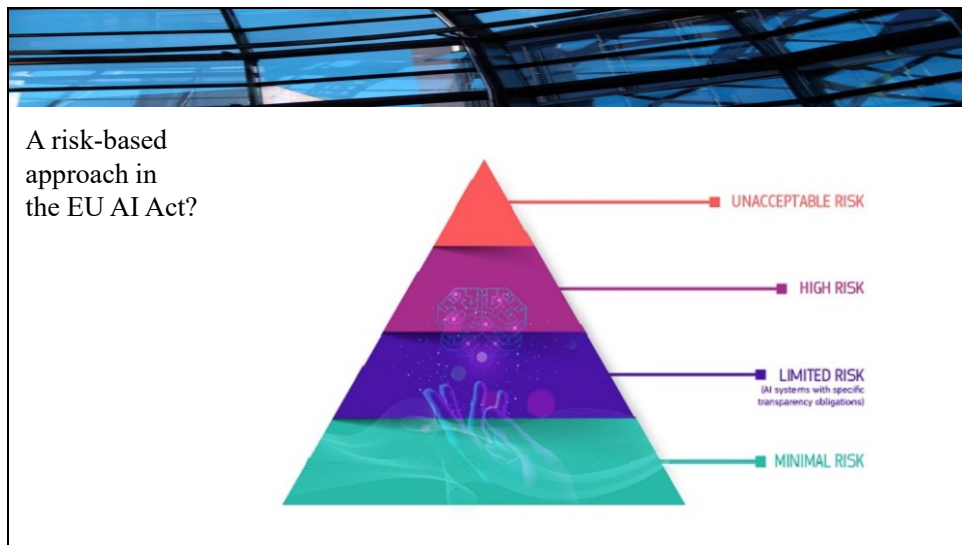


## EU AI Act

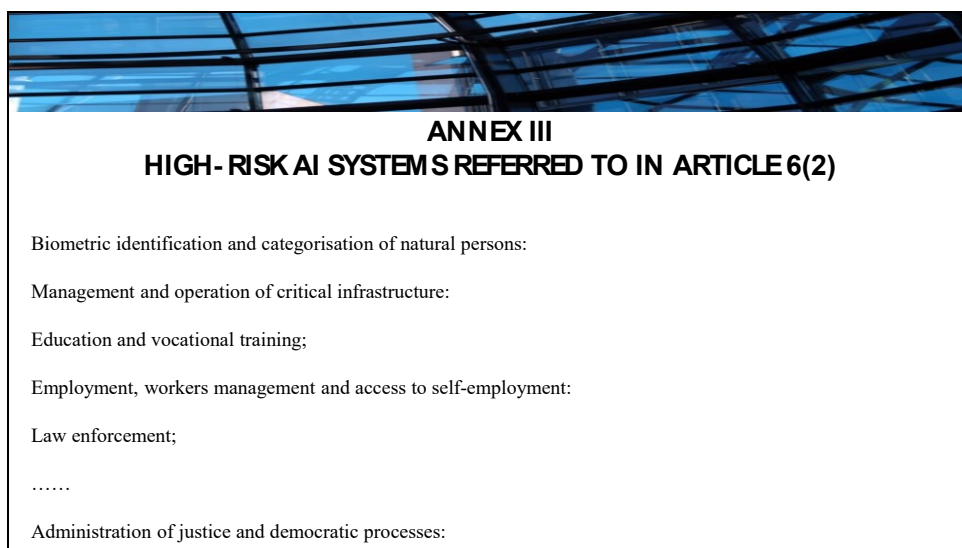
- The AI Act is a proposed European law on artificial intelligence (AI) – **the first law on AI** by a major regulator anywhere.
- Brussels, 21.4.2021
- The „GDPR“ of AI field
- <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>



18



19



20



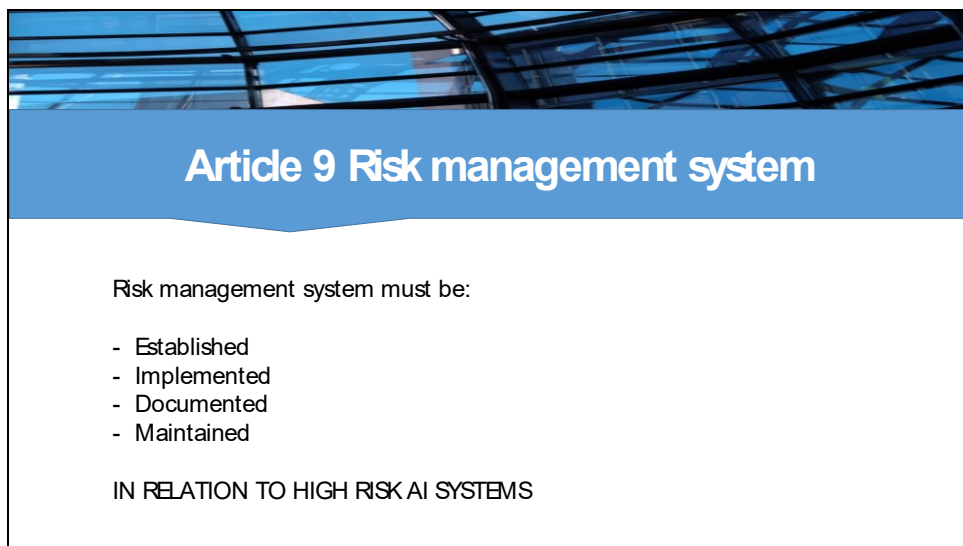
21

Risk classification for AI systems in different application scenarios		
Level	Application Scenarios	Constraint Strength
<b>Unacceptable risk</b>	All AI systems considered a clear threat to the safety, livelihoods and rights of people, such as social scoring by governments to toys using voice assistance that encourages dangerous behaviour.	<b>Absolutely forbidden</b>
<b>High risk</b>	<ul style="list-style-type: none"> <li>Critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;</li> <li>Safety components of products (e.g. AI application in robot-assisted surgery);</li> <li>Administration of justice and democratic processes (e.g. applying the law to a concrete set of facts). Etc.</li> </ul>	High-risk AI systems will be subject to <b>strict obligations</b> before they can be put on the market.
<b>Limited risk</b>	When using AI systems such as chatbots, users should be aware that they are interacting with a machine so they can take an informed decision to continue or step back.	Specific <b>transparency obligations</b> , such as clear and adequate information to the user.
<b>Minimal/ no risk</b>	AI-enabled video games or spam filters. The vast majority of AI systems currently used in the EU fall into this category.	<b>No intervention</b> implemented.

22



23



24






**Continuous process that runs during all the lifecycle of the high- risk AI system.**

- (a) identification and analysis** of the known and foreseeable risks associated
- (b) estimation and evaluation** of the risks that may emerge when the high- risk AI system is used
- (c) evaluation** of other possibly arising risks
- (d) adoption** of suitable risk management measures

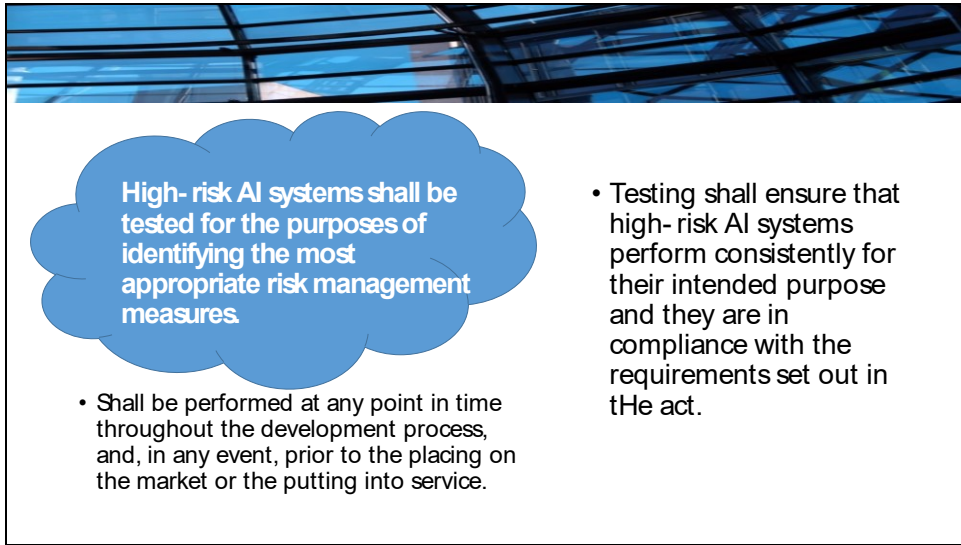
25



When identifying the best risk management measures, some measures should be ensured:

- Elimination and reduction of risks through adequate design and development
- Implementation of adequate mitigation and control measures
- Provisions of adequate information

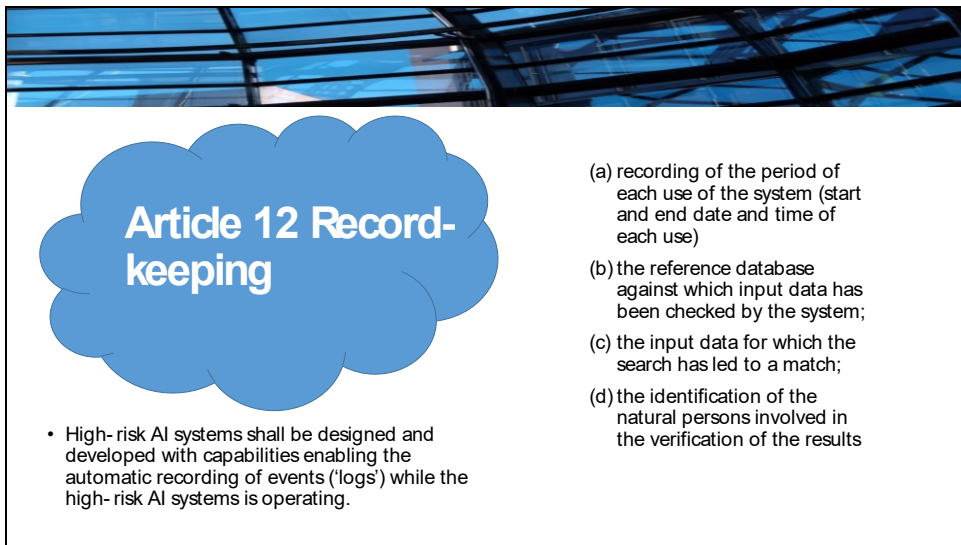
26



High-risk AI systems shall be tested for the purposes of identifying the most appropriate risk management measures.

- Shall be performed at any point in time throughout the development process, and, in any event, prior to the placing on the market or the putting into service.
- Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in the act.

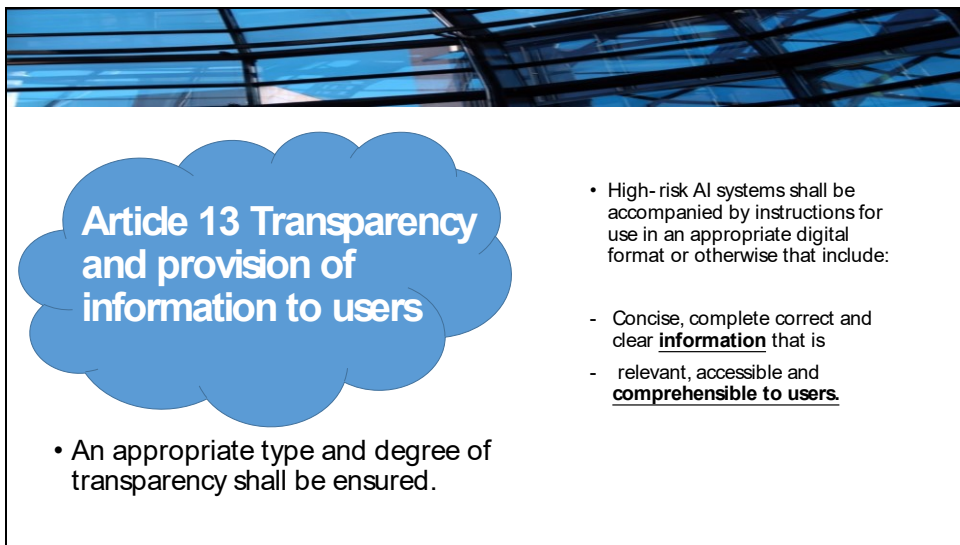
27



**Article 12 Record-keeping**

- High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating.
- (a) recording of the period of each use of the system (start and end date and time of each use)
- (b) the reference database against which input data has been checked by the system;
- (c) the input data for which the search has led to a match;
- (d) the identification of the natural persons involved in the verification of the results

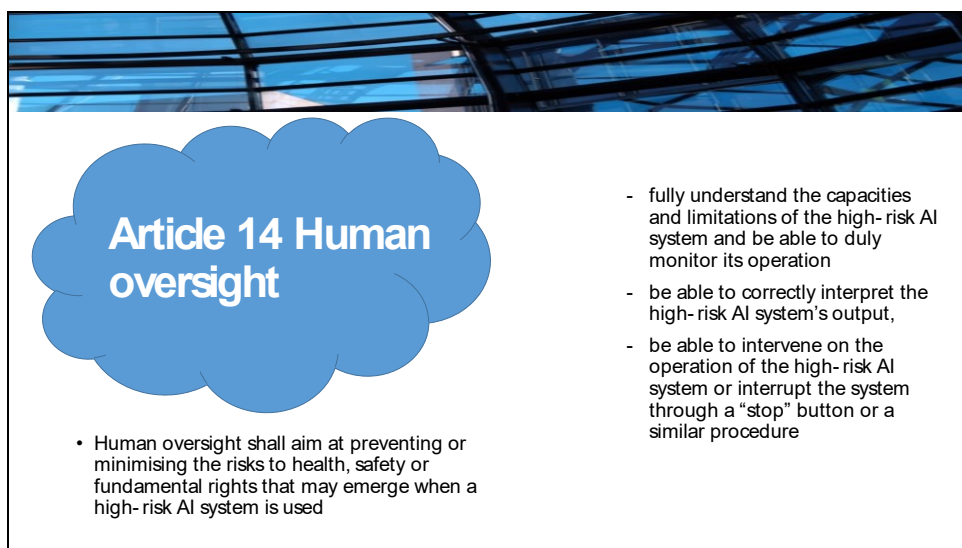
28



### Article 13 Transparency and provision of information to users

- An appropriate type and degree of transparency shall be ensured.
- High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include:
  - Concise, complete correct and clear **information** that is
  - relevant, accessible and **comprehensible to users.**


29



### Article 14 Human oversight

- Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used
- fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation
- be able to correctly interpret the high-risk AI system's output,
- be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure


30



### Article 16 Obligations of providers of high- risk AI systems

- (a) ensure that their high- risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;
- (b) have a **quality management system** in place which complies with Article 17;
- (c) draw- up the technical documentation of the high- risk AI system;
- (d) **keep the logs automatically generated** by their high- risk AI systems;
- (e) ensure that the high- risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;
- (f) comply with the **registration obligations** referred to in Article 51;
- (g) take the **necessary corrective actions**, if the high- risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title;
- (h) inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non- compliance and of any corrective actions taken;
- (i) to affix the CE marking to their high- risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;
- (j) upon request of a national competent authority, demonstrate the conformity of the high- risk AI system with the requirements set out in Chapter 2 of this Title.

31



### Article 17 Quality management system

- Providers of high- risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions,

32

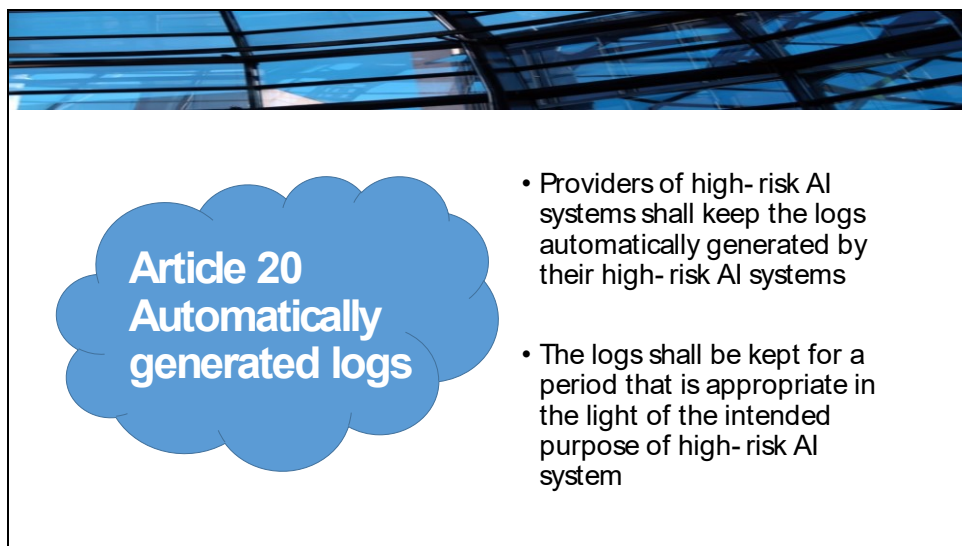


The slide features a blue cloud-shaped graphic on the left containing the text "Article 19 Conformity assessment". To the right of the cloud is a bulleted list. The top of the slide has a blue header image showing a glass and metal structure.

**Article 19 Conformity assessment**

- Providers of high- risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure

33



The slide features a blue cloud-shaped graphic on the left containing the text "Article 20 Automatically generated logs". To the right of the cloud are two bulleted list items. The top of the slide has a blue header image showing a glass and metal structure.

**Article 20 Automatically generated logs**

- Providers of high- risk AI systems shall keep the logs automatically generated by their high- risk AI systems
- The logs shall be kept for a period that is appropriate in the light of the intended purpose of high- risk AI system

34



## Article 21 Corrective actions

- Providers of high-risk AI systems which consider that a high-risk AI system is not in conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it.

35



## Article 22 Duty of information

- When the risk is known to the provider of the system, that provider shall immediately inform the national competent authorities of the Member States in which it made the system available.

36




**ENFORCEMENT**

- Regulation (EU) 2019/1020 (*market surveillance and compliance of products*) shall apply to AI systems covered by the act.

37



**An algorithm in the management board ?**



38



39



## III.

---

# Compliance

# Data Compliance

*Eylül Gürel, Attorney at Law (Turkey)*

*October 2022*

*Nicole Lima, Lawyer (Brazil), LL.B. (Amazonas, Brazil)*

*Thiti Sriwang, LL.B. (Thailand)*

## 1. Introduction

The main objective of this essay is to provide information about data compliance. This essay is structured as follows. The first part is data compliance. This part presents type of data compliance and what laws and/or regulations that a company should be aware to ensure that its business conduct adhering to such laws. The second part focus on data strategy for the company. This part will elaborate on data management, also focus on how the company can collect, transfer, secure, and store data. The last part focuses more on practical side. For example, reporting and documentation, customer experience and transparency, business contractual advantages and terms.

## 1. Data compliance

### 1.1. Business strategy and compliance

There are two definitions to keep in mind when it comes to compliance: Regulatory compliance and corporate compliance; the former is defined as the steps an organization takes to comply with relevant external laws, regulations, and guidelines, and the latter is defined as the actions and programs an organization sets in place to ensure compliance with internal policies, procedures, and accepted behavior, as well as external regulations. Organizations need to comply with both to ensure the security of their operations. Compliance functions through the steps of identifying the risks an organization faces, creating and implement processes to protect against those risks, monitoring and assessing the effectiveness of those risk-prevention processes, resolving compliance issues and advising the organization on better ways to minimize risk and comply with laws and regulations.

Identifying the risks an organization faces includes regularly running risk assessments, advising management on the areas that pose the biggest potential risks to the organization and reviewing audit results, recent litigation, compliance complaints, employee claims, industry enforcement trends, and policies in each risk area.

Creating and implementing processes to protect against those risks depends on the type of risk the organization is facing. Some risks may be unavoidable, but taking countermeasures always makes a difference, especially in the eyes of regulatory authorities. These countermeasures also involve revising existing policies and procedures, additional training / revamping the existing safety and security measures.

Monitoring and assessing the effectiveness of those risk-prevention processes is an ongoing process, changes are / should be made as problems arise. In this case, ensuring the internal controls actually help the organization comply with laws, regulations, and policies has utmost importance.

Resolving compliance issues means that the compliance officer should know the organization's policies and procedures backward and forward. They should be able to answer any questions about industry regulations and business laws. And they should also know the company's values, goals, and workplace culture. All of this together will help them ensure that the organization's operations are legal, ethical, and meet the highest level of compliance. In relation to this, advising the organization on better ways to minimize risk and comply with laws and regulations through following the updates and developments on laws, regulations, and industry standards helps secure the process of the insurance of the company's policy manual meeting those same requirements.

To summarize these points, compliance best practices can be listed as:

- Determine your end goals.
- Know your industry's regulatory environment.
- Create effective policies and procedures.
- Hold employees accountable.
- Conduct a compliance audit.
- Build a comprehensive document repository.
- Track violations (and costs).
- Compliance training.
- Communicate clearly and regularly.
- Regularly review your compliance program.

## **1.2. Law and Regulation relating to Data Compliance**

Every country has enacted some sort of data protection/compliance laws to regulate how information is collected, how data subjects are informed, and what control a data subjects have over their information once it is transferred. Failure to follow such laws may lead to fines, lawsuits, and even prohibition of a site's use in certain jurisdictions.

This topic presents some of the European laws and regulations relating to data compliance.<sup>34</sup>

### *The General Data Protection Regulation (GDPR)*

The most important data protection legislation enacted to date is the General Data Protection Regulation (GDPR). It governs the collection, use, transmission, and security of data collected from residents of any of the 28 member countries of the European Union. The law applies to all EU residents, regardless of the entity's location that collects the personal data. Fines of up to € 20 million or 4% of total global turnover may be imposed on organizations that fail to comply with the GDPR.

### *The Data Act*

The Data Act is a key pillar of the European strategy for data. It will make an important contribution to the digital transformation objective of the Digital Decade. The Data Act will ensure fairness by setting up rules regarding the use of data generated by Internet of Things (IoT) devices.

Users of objects or devices generally believe that they should have full rights of the data they generate. However, these rights are often unclear. And, manufacturers do not always design their products in a way that allows users, both professionals and consumers, to take full advantage of the digital data they create when using IoT objects. This leads to a situation where there is no fair distribution of the capacity to build on such important digital data, holding back digitisation and value creation.<sup>35</sup>

### *The Digital Service Act and Digital Markets Act*

The European Commission proposed two legislative initiatives to upgrade rules governing digital services in the EU: the Digital Services Act (DSA) and the Digital Markets Act (DMA). Together they form a single set of new rules that will be applicable across the whole EU to create a safer and more open digital space. The DSA and DMA have two main goals: (1) to create a safer digital space in which the fundamental rights of all users of digital services are protected; and (2) to establish a level playing field to foster

---

<sup>34</sup> 'Data privacy laws: What you need to know in 2022' (*Osano Staff*, 4 July 2022) <<https://www.osano.com/articles/data-privacy-laws> > accessed 16 October 2022.

<sup>35</sup> 'Data Act' (*European Commission*, 7 July 2022) <<https://digital-strategy.ec.europa.eu/en/policies/data-act> > accessed 16 October 2022.

innovation, growth, and competitiveness, both in the European Single Market and globally.<sup>36</sup>

### *Artificial Intelligence Act*

The EU's Artificial Intelligence Act would apply to any company doing business in the EU that develops or adopts machine-learning-based software. The Act was introduced last year and is moving through the review process. It would apply extraterritorially, meaning the law will cover companies based elsewhere if they have customers or users inside the EU and effectively making it a global regulation.

### *E-Privacy Regulation*

The e-Privacy Regulation (ePR) has been a long time coming. It aimed to come into force alongside the EU's General Data Protection Regulation in 2018 but has stalled for years. In March 2022, the EU Council agreed on a draft, but regulation isn't expected until at least 2023.

The e-Privacy Regulation, if passed, would create privacy rules for traditional electronic communications services and entities that weren't covered by the former law, the e-Privacy Directive, such as WhatsApp, Facebook Messenger, and Skype.

## **1.3. Requirements and grounds/legal basis for data-GDPR articles**

This topic can be divided into two categories, GDPR Article 6 Lawfulness of Processing and GDPR Article 9 Processing of Special Categories of Personal Data.

### *Lawfulness of Processing*

For a data processing operation to be considered lawful, one has to obtain the consent of the data subject (which has to be free, informed, specific, unambiguous) or have another legitimate ground provided. Article 6 (1) of the GDPR foresees five lawful grounds for processing, in addition to consent, i.e. when processing personal data is necessary for the performance of a contract, for the performance of a task carried out in the exercise of public authority, for compliance with a legal obligation, for the purpose of the legitimate interests of the controller or third parties, or if necessary to protect the

---

<sup>36</sup> 'The Digital Services Act package' (European Commission, 12 October 2022) <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>> accessed 16 October 2022.

vital interests of the data subject. However, these legitimate grounds are limited to non-sensitive personal data.

### *Processing of Special Categories of Personal Data*

EU law has a regime for processing special categories of data (also called 'sensitive data'). These reveal racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership as well as for processing genetic and biometric data for the purposes of uniquely identifying a natural person, and for data concerning health, a person's sex life or sexual orientation. The processing of sensitive data is prohibited in principle, however an exhaustive list of exemptions to this prohibition can be found in Article 9 (2), which amount to lawful grounds for processing sensitive data:

- the data subject explicitly consents to the data processing;
- processing is carried out by a non-profit body with political, philosophical, religious or trade union purposes in the course of its legitimate activities and only relates to its (former) members or to persons who have regular contact with it for such purposes;
- processing concerns data explicitly made public by the data subject;
- processing is necessary:
  - to carry out the obligations of, and to exercise the specific rights of, the controller or of the data subject in the employment, social security and social protection context;
  - to protect the vital interests of the data subject or another natural person (when the data subject cannot give consent);
  - to establish, exercise or defend legal claims or when courts act in their judicial capacity;
  - for preventative or occupational medicine purposes: "for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional";
  - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
  - for public interest reasons in the area of public health; or
  - for substantial public interest reasons.

To process special categories of data, a contractual relationship with the data subject is thus not viewed as a legal basis for the legitimate processing of sensitive data, except for a contract with a health professional subject to the obligation of professional secrecy.

GDPR provides that sensitive data can be processed where processing is necessary for:

- preventative or occupational medicine purposes, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of EU or Member State law, or pursuant to a contract with a health professional;
- reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or Member State law. The law must provide for suitable and specific measures to safeguard the rights of the data subject;
- archiving, scientific or historical research or statistical purposes on the basis of Union or Member State law. The law must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to safeguard the rights and interests of the data subject.

For more detailed information and examples, please refer to Handbook on European data protection law, 2018 edition.

#### **1.4. Chief Data Officer and Data Protection Officer**

This part will focus on the person who is usually responsible for data compliance. Usually, many positions play the role in the data compliance. But this essay will focus mainly Chief Data Officer (CDO) and Data Protection Officer (DPO).

##### *Chief Data Officer (CDO)*

The chief data officer (CDO) is a senior executive responsible for the utilization and governance of data across the organization. While the chief data officer title is often shortened to CDO, the role should not be confused with that of the chief digital officer, which is also frequently referred to as CDO.

The CDO is responsible for a firm's enterprise-wide data and information strategy, governance, control, policy development, and effective exploitation. Chief Data Officer responsibilities include: (1) Governance: Advising on, monitoring, and governing enterprise data (2) Operations: Enabling data usability, availability, and efficiency (3) Innovation: Driving enterprise digital transformation innovation, cost reduction, and revenue generation and (4) Analytics: Supporting analytics and reporting on products, customers, operations, and markets.

### *Data Protection Officer (DPO)*

The primary role of the data protection officer is to ensure that his/her organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. The appointment of a DPO must of course be based on his/her personal and professional qualities, but particular attention must be paid to his/her expert knowledge of data protection. A good understanding of the way the organisation operates is also recommended.<sup>37</sup>

### **1.5. IP-databases**

Once a company has collected enough data to form a database, two (or rather three) options can be followed to protect it under intellectual property:

- Sui Generis Protection, Article 7 (1) and (2) of the Directive 96/9/EC (“Database Directive”), substantial investment
- Copyright Protection, creative input in structure
- RyanAir - C-30/14, Contractual limitations: Providers of data that are not protected by copyright or database rights under the Directive are free to impose contractual limitations on their use

When collecting data from the internet, private entities such as companies, have to be careful about the usage of the following due to their license conditions (and avoid the “infectious” licenses): Creative Commons, Open Source Software.

For more information, please refer to: Less Is More? Protecting Databases in the EU After Ryanair by Matěj MYŠKA, Jakub HARAŠTA; DOI 10.5817/MUJLT2016-2-3.

## **2. Data Strategy**

### **2.1. Management**

Data management is the practice of collecting, keeping, and using data securely, efficiently, and cost-effectively. The goal of data management is to help organizations optimize the use of data within the bounds of policy and regulation so that they can

---

<sup>37</sup>. ‘Data Protection Officer (DPO)’ <[https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo\\_en#:~:text=The%20primary%20role%20of%20the,the%20applicable%20data%20protection%20rules](https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en#:~:text=The%20primary%20role%20of%20the,the%20applicable%20data%20protection%20rules)> accessed 16 October 2022.



make decisions and take actions that maximize the benefit to the organization. The data management may be managed in cooperation between the IT department and the Chief Data Officer (CDO) if it is being managed in-house, or it can be managed by the service provider. The 'who' is ultimately less important, so long as the data is appropriately managed in accordance with data regulations and in alignment with business requirements.

Making a data management plan and organizing your data from the beginning of your project will save you enormous time, money, and energy. A Data Management Plan consists of many elements describing the preservation, sharing, and access for your data. When it comes to managing data and documents within a workgroup, you must implement processes that work best for your team. Even if you are in the middle of a project, a good place to start is to define directory structures and naming conventions. Defining structure early in the process provides an organizational foundation for all your data and document files. Best practices for setting up prior to data collection include:

- Establishing Naming Conventions for your files and using them consistently will ensure maximum access to your data and records
- Building Directory Structures refers to the method of classifying and organizing data sets to make them more useful.
- Using a system for active project Version Control can help keep track of all sorts of files, including text documents and analysis code.
- Creating plain text or README Files that contain information about other files in a folder for each distinct dataset.

## 2.2. Collection

Data collection is an important phase of Data Strategy, it is actually the second step after the generation of data.<sup>38</sup> The collection is the process of gathering, measuring, and analyzing complete and accurate data for the organization's decision-making process.<sup>39</sup> During this phase, it is essential to ensure data is collected legally and ethically, therefore, it must be compliant with current data protection regulations and guidelines.<sup>40 41</sup>

---

<sup>38</sup> '7 Data Collection Methods in Business Analytics' (*Business Insights Blog*, 2 December 2021) <<https://online.hbs.edu/blog/post/data-collection-methods>> accessed 16 October 2022.

<sup>39</sup> 'What Is Collection of Data? Methods, Types & Everything You Should Know' (*Simplilearn.com*, 13 May 2021) <<https://www.simplilearn.com/what-is-data-collection-article>> accessed 16 October 2022.

<sup>40</sup> '7 Data Collection Methods in Business Analytics' (*Business Insights Blog*, 2 December 2021) <<https://online.hbs.edu/blog/post/data-collection-methods>> accessed 16 October 2022.

<sup>41</sup> 'Data Collection: Methods, Challenges and Key Steps' (*SearchCIO*) <<https://www.techtarget.com/searchcio/definition/data-collection>> accessed 16 October 2022.

A considerable portion of the data collected by companies goes unused, so a lot of valuable data go to waste. That is why a data management strategy is so relevant, in a way that there will be data traceability.<sup>42</sup>

There are five components to this part of the strategy: Own, who will be the one responsible for your strategy; Explain, why you collect, which use cases and the value for the data collected, to define data goals and align it to business strategy; Plan, create a standardization and traceability to ensure quality and consistency in the data collection, it is how data will be easily consolidated for use; Categorize, it is the part where there is organization of categories of data process and utilization of tools; and, Analyze, through defined metrics the business strategy tools will analyze the data collected. These components are essential to keeping it all organized and prepared for next steps as storage, transfers, security and transparency.<sup>43</sup>

In this collection can be some types of data: First-party data, which is collected directly from users by the organization; Second-party data, which is data shared by another organization about its customers; and Third-party data, which is data that has been aggregated or sold by organizations.<sup>44</sup>

The incorrect collection can cause consequences as wrong conclusions that take to poorly made decisions, which can harm parties. In this respect, there should be an error detection process in the strategy for quality control and assurance.<sup>45</sup> This way data quality will be guaranteed, bringing trust and reliability to the data collected, which result in satisfactory analysis and informed decisions.<sup>46</sup>

### 2.3. Transfer

Data Transfer is also a common step for the data strategy. In this part, it needs safeguards to ensure that data is not misused, including outside Europe.<sup>47</sup>

In this matter, European Union has a digital and data strategy with the Digital Market Act, the Digital Services Act, the Data Governance Act and the Data Act, to regulate data

---

<sup>42</sup> 'How A Data Strategy Framework Simplifies Data Collection | Twilio Segment' (*Segment*) <<https://segment.com/resources/data-strategy/Data-Strategy-Framework-Can-Make-Data-Collection-Simple/>> accessed 16 October 2022.

<sup>43</sup> 'How A Data Strategy Framework Simplifies Data Collection | Twilio Segment' (*Segment*) <<https://segment.com/resources/data-strategy/Data-Strategy-Framework-Can-Make-Data-Collection-Simple/>> accessed 16 October 2022.

<sup>44</sup> '7 Data Collection Methods in Business Analytics' (*Business Insights Blog*, 2 December 2021) <<https://online.hbs.edu/blog/post/data-collection-methods>> accessed 16 October 2022.

<sup>45</sup> 'What Is Collection of Data? Methods, Types & Everything You Should Know' (*Simplilearn.com*, 13 May 2021) <<https://www.simplilearn.com/what-is-data-collection-article>> accessed 16 October 2022.

<sup>46</sup> Snowplow Team, 'Why Data Collection Is Key to Your Data Strategy - Part One' (*Snowplow*, 25 February 2020) <<https://snowplow.io/blog/why-data-collection-is-key-to-your-data-strategy-part-one/>> accessed 16 October 2022.

<sup>47</sup> EPIC, 'Data Transfers in the Data Strategy: Understanding Myth and Reality' (*DIGITALEUROPE*) <<https://www.digitaleurope.org/resources/data-transfers-in-the-data-strategy-understanding-myth-and-reality/>> accessed 16 October 2022.

by the side of GDPR. This strategy aims to make EU a data-driven society, in a way to allow secure free data flow in EU and outside it across sectors.<sup>48</sup>

Also, data transfer has a goal to enhance performance and competitiveness, but can be a risk process, as it involves change in storage or database, moving data from one system to another.

The data integration and data migration need to be well-established through a plan, this should contain knowledge of the data and audit, cleanup to resolve any issues, maintenance to maintain data quality, protection to secure reliability on data, and governance to track and report data integrity. In addition, there is the need to have right software and tools for step-by-step plan procedure into the business strategy. Lastly, to safely do the process, it is always advised to execute a backup of the data.<sup>49</sup>

## 2.4. Storage

Data storage is the retention of information using technology specifically developed to keep that data and have it as accessible as necessary. Data storage refers to the use of recording media to retain data using computers or other devices. The most prevalent forms of data storage are file storage, block storage, and object storage, with each being ideal for different purposes. When it comes to managing data storage, many companies face a difficult set of compromises. Data must be accessible, but it must also be kept securely. Cloud data storage is far more cost efficient than on-premises storage, but it can make compliance with data security standards more difficult, and more expensive. the best practice for data storage includes:

- Document actions (having some sort of explanatory information regarding storage policy to support the appropriateness of choices, if ever audited.)
- Using tools to implement and automate governance of data
- Making sure the data is stored on the most cost-effective and basic policy and access requirements are met
- Anonymize data (data that is subject to regulation can be anonymized, so it no longer runs afoul of regulations such as GDPR, enabling retention to continue but with less risk.)

## 2.5. Security

---

<sup>48</sup> 'European Data Strategy' (*European Commission - European Commission*) <[https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en)> accessed 16 October 2022.

<sup>49</sup> 'Data Migration: Strategy and Best Practices' (*Talend - A Leader in Data Integration & Data Integrity*) <<https://www.talend.com/resources/understanding-data-migration-strategies-best-practices/>> accessed 16 October 2022.

This part will focus on how to prevent cybersecurity incident. First of all, it is better to understand that you cannot prevent all incidents. Cybersecurity incidents will happen, it is a matter of time. In addition, cybersecurity incidents are detected late. Therefore, prevention is rarely an option after detection. The best practice that you can do conclude:

- **Keep Key Stakeholders in the Loop:** Make sure the key stakeholders understand your data protection strategy and approve of it. This will help ensure that employees comply with the strategy and apply data protection across the organization, not just relegating it to IT.
- **Keep Track of All Available Data:** Make a data inventory that encompasses all information your organization stores or processes. by your organization. You have to understand your data in order to protect it—take note of the type of data collected, its storage location, usage and sharing policies. This allows you to map your data systems and facilitate management.
- **Conduct a Risk Analysis:** Some regulations require companies to proactively identify risks and take measures to mitigate them. Risk assessments are essential for making your organization accountable and allowing you to identify potential threats or deficiencies. Your business infrastructure is a complex web, with many pathways for transferring data—each pathway poses a potential risk, and you must protect the data even when being used by a third party. Perform a risk analysis to identify individual risks across your network. This will help inform your data protection policies.

### **3. Practical side**

#### **3.1. Reporting and documentation**

**Information & Notification Obligations:** For the data subject, GDPR Articles 12, 13, 14, 19; for the authorities, GDPR Articles 30, 33.

Article 12 of the GDPR establishes a broad comprehensive obligation for controllers in providing transparent information and/or communicating how data subjects can exercise their rights. The information must be concise, transparent, intelligible and easily accessible, using clear and plain language. It must be provided in written form, including electronically where appropriate, and it may even be provided orally at the data subject's request and if his or her identity is proven beyond doubt. The information shall be provided without excessive delay or expense. Article 13 and Article 14 of the GDPR deal with the right of data subjects to be informed, either in situations where personal data were collected directly from them, or in situations where the data were not

obtained from them, respectively. Article 19 is in relation to Articles 16 (rectification), 17 (erasure), 18 (restriction of processing) and foresees a notification obligation regarding rectification or erasure of personal data or restriction of processing.

A personal data breach refers to a security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to processed personal data. The causes of data breaches may range from accidental mistakes by people working inside an organization to external threats such as hackers and cybercriminal organizations.

In addition to the obligation to take measures to ensure the security of processing, it is equally important to ensure that when breaches occur, controllers address them in an appropriate and timely manner. Accordingly, controllers must notify certain data breaches to the supervisory authorities without undue delay and, where feasible, within 72 hours of the moment they become aware of the breach. If they exceed the 72-hour timeframe, the notification needs to be accompanied with an explanation for the delay. Controllers are exempt from the notification requirement only where they are able to demonstrate that the data breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned.

The regulation specifies the minimum information to be included in the notification to allow the supervisory authority to take the necessary action. The notification must include, at least, a description of the nature of the data breach and of the categories and approximate numbers of data subjects affected, a description of the possible consequences of the breach and of the measures implemented by the controller to address and mitigate its consequences. In addition, the name and contact details of the data protection officer or another contact point should be provided, to enable the competent supervisory authority to obtain further information if necessary.

If a data breach is likely to cause high risks to the rights and freedoms of individuals, controllers must inform these individuals (the data subjects) of the breach without undue delay. The information to the data subjects, including the description of the data breach, must be drafted in clear and plain language, and include information similar to that required for notifications to supervisory authorities. In certain circumstances, controllers may be exempt from the obligation to notify data subjects of such breaches. Exemptions apply where the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption. Action taken by the controller after the breach to ensure that the harm to the rights of data subjects will no longer materialize may also exempt the controller from the obligation to notify the data subjects. Finally, if notification entails disproportionate

effort on behalf of the controller, data subjects can be informed about the breach through other means, such as a public communication or similar measures.

The obligation to notify data breaches to the supervisory authorities and data subjects is addressed to controllers. However, data breaches may occur irrespective of whether processing is carried out by a controller or processor. For this reason, it is essential to ensure that processors are also required to report data breaches. In this case, processors must notify data breaches to the controller without undue delay. The controller is then responsible for notifying the supervisory authorities and the data subjects affected, subject to the aforementioned rules and timeframe.

### 3.2. Customer experience and transparency

After preparing and ensuring that the documentation of every step of the data strategy is clear and complete, it is possible to elaborate a data transparency status. This ensures that data is being used with integrity, lawfully, fairly, traceability, and for valid purposes.<sup>50</sup>

Through the establishment of data transparency, customer experience can be enhanced. The development of customer trust is the result of the implementation of this characteristic. In which it is included integrity and security in all stages of processing data.<sup>51</sup>

This is relevant in the customer experience because it means that data will be easily accessible and understandable. The clarity of this data through that path increases trust, allows for better decision-making, and promotes accountability.<sup>52</sup>

Some actions that are inside such data transparency is to only collect the necessary data, keep clients informed, map data processing, establish a data transparency policy and comply with regulations.<sup>53</sup>

+ + +

---

<sup>50</sup> Gatekeeper, 'Data Transparency - Definition'

<<https://www.gatekeeperhq.com/glossary/data-transparency>> accessed 16 October 2022.

<sup>51</sup> Timothy Morey, Theodore "Theo" Forbath and Allison Schoop, 'Customer Data: Designing for Transparency and Trust' [2015] *Harvard Business Review* <<https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>> accessed 16 October 2022.

<sup>52</sup> 'Why Data Transparency and Traceability Matter in Sustainability?'

<<https://sustainlab.co/blog/why-data-transparency-and-traceability-matter-in-sustainability>> accessed 16 October 2022.

<sup>53</sup> 'How To Ensure Data Transparency - DZone Big Data' (*dzone.com*)

<<https://dzone.com/articles/how-to-ensure-data-transparency-and-why-its-import>> accessed 16 October 2022.



1



2

## Data Compliance

### Functions of compliance

- ▶ Identify the risks an organization faces
- ▶ Create and implement processes to protect against those risks
- ▶ Monitor and assess the effectiveness of those risk-prevention processes
- ▶ Resolve compliance issues
- ▶ Advise the organization on better ways to minimize risk and comply with laws and regulations

3

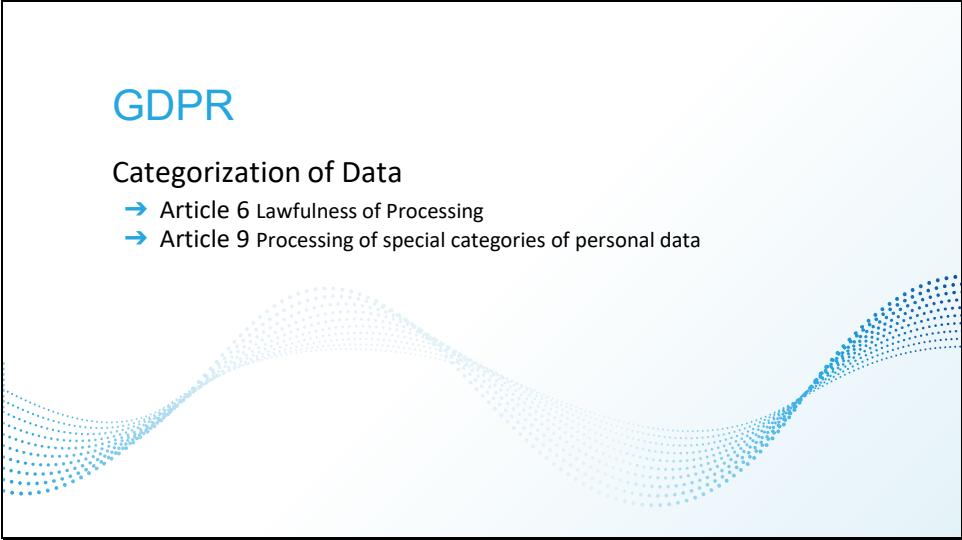
## Data Compliance

### Compliance Best Practices

- ▶ Determine your end goals.
- ▶ Know your industry's regulatory environment.
- ▶ Create effective policies and procedures.
- ▶ Hold employees accountable.
- ▶ Conduct a compliance audit.
- ▶ Build a comprehensive document repository.
- ▶ Track violations (and costs).
- ▶ Compliance training.
- ▶ Communicate clearly and regularly.
- ▶ Regularly review your compliance program.

4



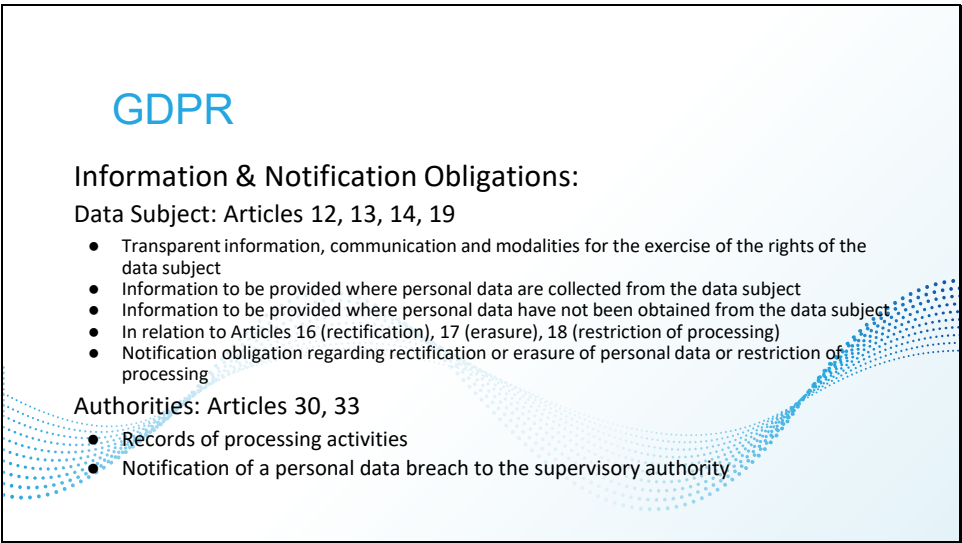


## GDPR

### Categorization of Data

- Article 6 Lawfulness of Processing
- Article 9 Processing of special categories of personal data

5



## GDPR

### Information & Notification Obligations:

Data Subject: Articles 12, 13, 14, 19

- Transparent information, communication and modalities for the exercise of the rights of the data subject
- Information to be provided where personal data are collected from the data subject
- Information to be provided where personal data have not been obtained from the data subject
- In relation to Articles 16 (rectification), 17 (erasure), 18 (restriction of processing)
- Notification obligation regarding rectification or erasure of personal data or restriction of processing

Authorities: Articles 30, 33

- Records of processing activities
- Notification of a personal data breach to the supervisory authority

6

## Data Compliance

### Data Protection Officer

- The primary role of the data protection officer is to ensure that his/her organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.
- The appointment of a DPO must of course be based on his/her personal and professional qualities, but particular attention must be paid to his/her expert knowledge of data protection. A good understanding of the way the organisation operates is also recommended.

7

## IP

### Databases

- Sui Generis Protection, Article 7 (1) and (2) of the Directive 96/9/EC (“Database Directive”), substantial investment
- Copyright Protection, creative input in structure
- RyanAir - C-30/14, Contractual limitations: Providers of data that are not protected by copyright or database rights under the Directive are free to impose contractual limitations on their use

8

## IP

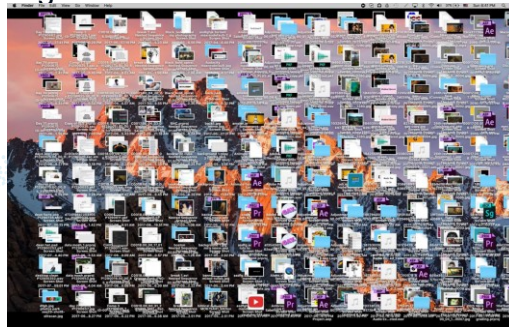
Creative Commons, OSS and other sources of data to beware

- Following licensing terms
- Avoiding «infectious» licenses

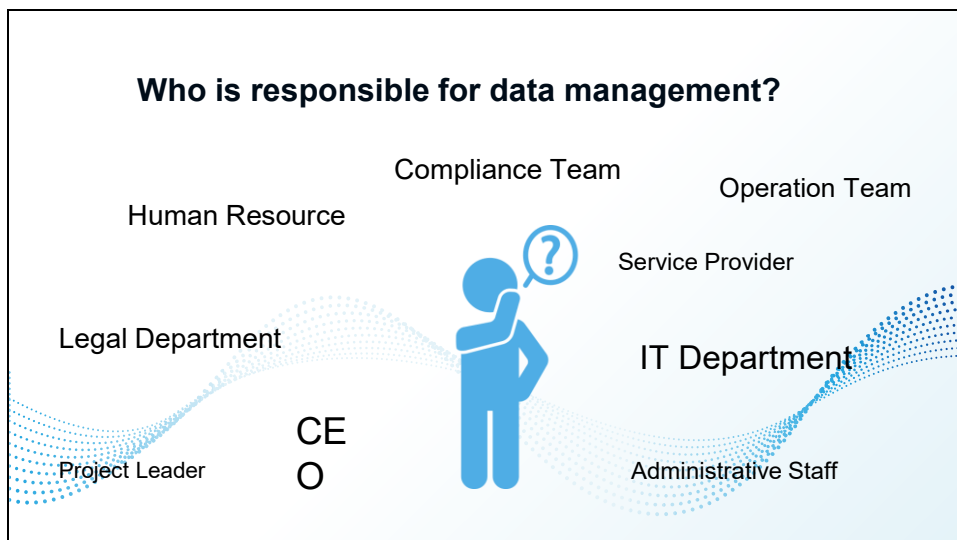
9

## Data Strategy

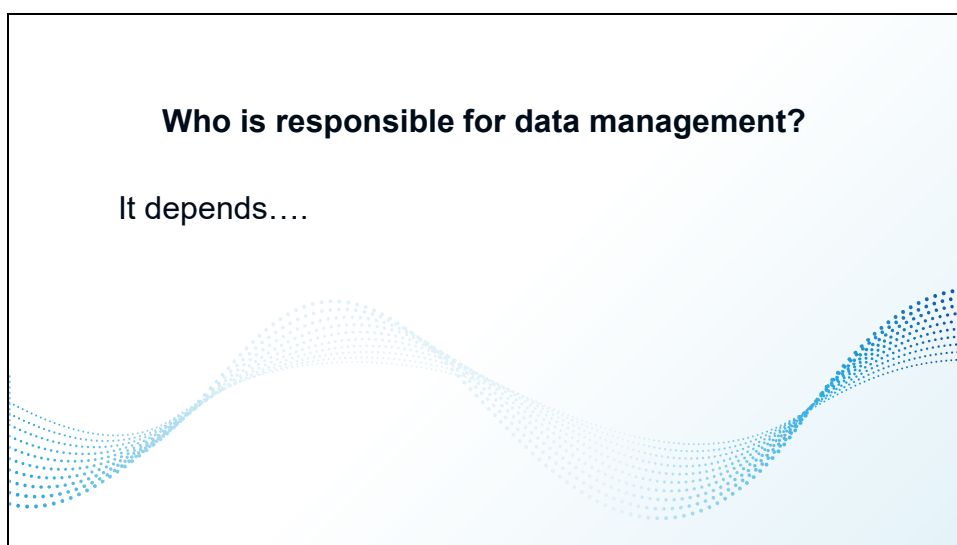
Data Management



10



11



12

## Chief Data Officer (CDO)

- *businesses that have a CDO are twice as likely to have a clear digital strategy.*
- *two-thirds of such firms say they are outperforming rivals in market share and data-driven innovation*
- *have more security and confidence that data is constantly being monitored for accuracy.*

13

## Data Management Plan

Consists of many elements describing the preservation, sharing, and access for organization's data.

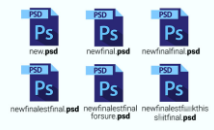
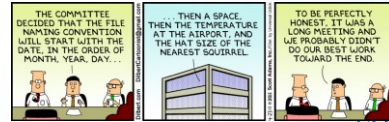
Before collection of data, it is good to **generate the structure.**

14

## Data Management Plan

### Structure Generation

- Establishing Naming Conventions
- Building Directory Structures
- Using a Version Control Software
- Creating plain text or README Files



15

## Data Strategy

### Data Collection

- Second step, after generation
- More than 50% of the data collected by companies goes unused. That means companies are letting a lot of valuable data go to waste
- Data collection is the process of gathering, measuring, and analyzing accurate data for the decision-making
- Data strategy fills in the cracks by keeping track of all the data you're collecting, why you're collecting data, what you're doing with it, and who is in charge of it
- Own, Explain, Plan, Categorize and Analyze
- First, second, and third-party data
- When collecting data, it must be compliant with current Data Protection laws

16

## Data Strategy

### Data Transfer

- Safeguards to ensure that data is not misused, including outside Europe
- EU's digital and data strategy: the Digital Market Act, the Digital Services Act, the Data Governance Act and the Data Act, besides GDPR
- Data integration and data migration need to be well-established through a plan
- Knowing the data, Cleanup, Maintenance, Protection and Governance
- Right software and tools for step-by-step procedure

17

## Data Strategy

### Data Storage

When it comes to managing data storage, many companies face a difficult set of compromises. Data must be accessible, but it must also be kept securely. Cloud data storage is far more cost efficient than on-premises storage, but it can make compliance with data security standards more difficult, and more expensive. the best practice for data storage includes:

- Document actions (having some sort of explanatory information regarding storage policy to support the appropriateness of choices, if ever audited.)
- Using tools to implement and automate governance of data
- Making sure the data is stored on the most cost-effective and basic policy and access requirements are met
- Anonymize data (data that is subject to regulation can be anonymized, so it no longer runs afoul of regulations such as GDPR, enabling retention to continue but with less risk.)

18

## Data Strategy

### Data Security- How to prevent cybersecurity incidents?

- you cannot prevent (all of them).

what you can do is...

- to minimise the legal, financial and reputational consequences after an incident
- to improve the evidence of prevention

19

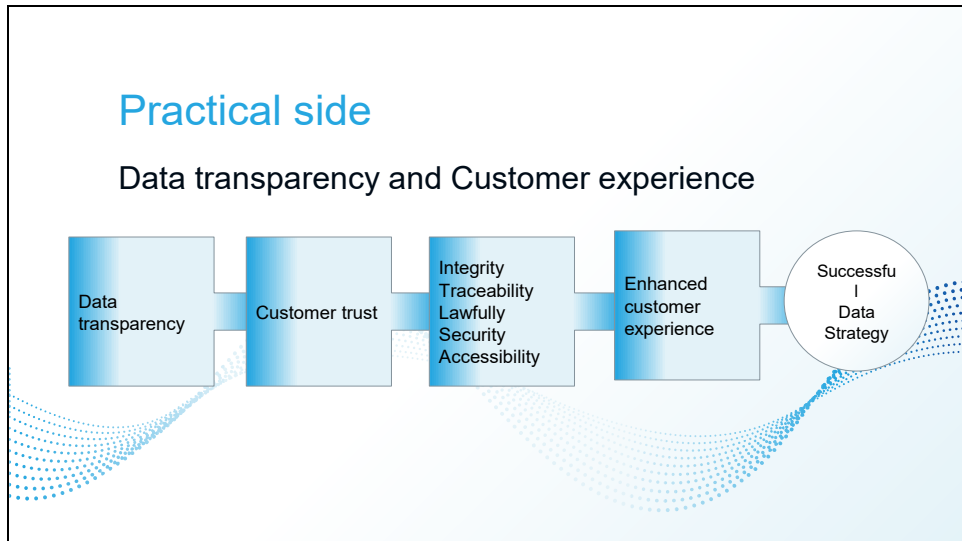
## Data Strategy

### Data Security- How to prevent cybersecurity incidents?

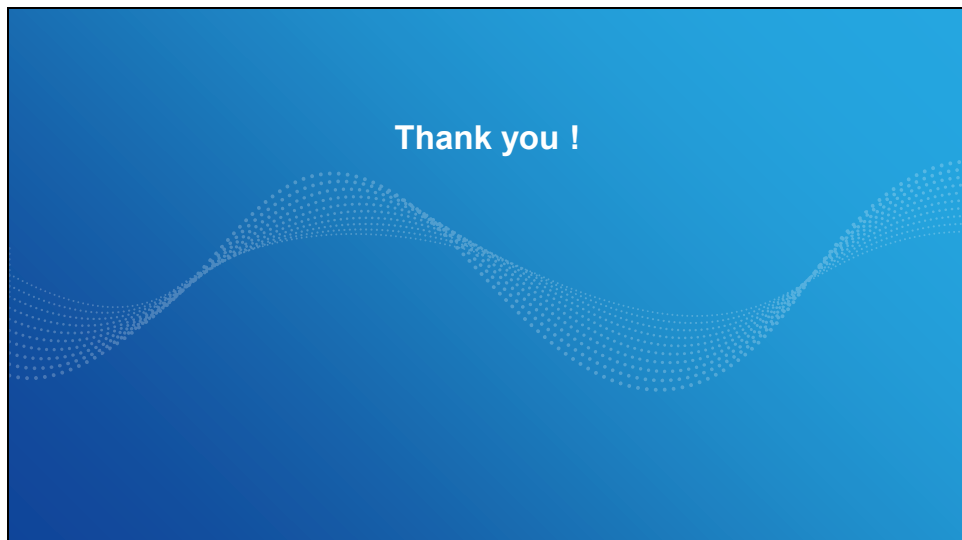
- Build your relationship with the security team
- Understand the most common sources of incidents for your company
- Understand how incidents occur
- Understand the options to prevent incidents
- Move the options forward to implementation

20





21



22

## IV.

---

# Due Diligence

# Due Diligence on IT, Security, Data and Data Protection

*Mustafa Enes Balin, Attorney at Law (Turkey)*

*October 2022*

*Irem Atik, Attorney at Law (Turkey)*

*S. J. Jagannadh Palepu, LL.B. (India)*

## **Abstract**

Mergers and Acquisitions has become a crucial tool for furthering the business expansions. Every business looks to innovate and expand to other markets to demonstrate its presence in the market and gain profits. The latin doctrine ‘caveat emptor’ which translates to “Let the buyer beware” is apt in M&A as well. Only the buyer is responsible for checking the quality and suitability of the goods before making the purchase. Similarly, the acquirer of a business has to do the necessary homework on the target company i.e the due diligence which is conducted internally for the purposes of knowledge and awareness and risk analysis. Access to data and control over data has also become a yardstick to measure the company’s presence and success in terms of relevant markets. The due diligence also includes a data aspect which scrutinizes the issues related to data ownership, security, privacy and transfers between the merging businesses. In this backdrop, this report provides a toolkit to the readers, stakeholders on how to tackle the key considerations when conducting a due diligence on data, IT and Data protection issues during a merger.

The first part deals with the due diligence and data related issues following up with IT security due diligence which deals with key aspects to be considered in cyber due diligence and lastly the report addresses the Data privacy and protection issues in mergers.

## **1. Data due diligence**

Many companies tend to try merger and acquisition process in order for their growth to increase due to the fact that other growth component is insufficient to extend their volume. M&A process could be accomplished two ways: strategic or financial. On the strategic level, companies could cut costs by combining process, property or personnel. On the financial level, it is led by a group of investors, such as private equity companies, which is a type of alternative investment in which the investors purchase shares in

privately-held business. Otherwise strategic buyers, they would like to make a further step to sell at a higher price in the future.

Nevertheless, this undertaking cannot be as easy as on paper because of non-intended results. Some of them produce higher cost than expected or lower returns than acceptable. Non-intended results means losses of value for shareholders of the acquiring company, even though it could make a benefit for targeting the company's shareholders after M&A.

To prevent these unintended results, then to increase the possibilities of achievement of M&A process, there has to be one solution so that companies would not give up M&A process despite unintended results, that is, *due diligence*.

### **1.1. When is Due Diligence On The Table**

Acquirer could only have general familiarity, not could reach a crucial data regarding targeted company. This situation makes acquirer depend on merely assumptions which could bring naturally failure. Due diligence is a important tools in order to prevent such failures by looking closely. Ultimately, acquirer gain comfort that a target company is what it is represented to be in addition validates key assumptions and mitigates the risk that acquisition will bring bring unwelcome surprises.

Companies that use due diligence generally perform many activities to understand previously what is the current condition of the target company. It needs a professional team of not only internal but also external experts. During the specified pre-contractual period, that team strives to discover as much as possible regarding the true statement and future prospects of business by accessing the company. Thus, the acquirer could have an idea before the deal. This situation gives an opportunity that previously search undisclosed risks, support or alter valuation and then provide input for prospective negotiation of M&A agreements.

### **1.2. What is the Data Diligence**

With the advance of Big Data, a new manner has emerged around data analyses during M&A. To understand better, basically hardly every company is directly related, greater or lesser extent, somehow data. It also affect surely M&A process. After that point, M&A process has driven to a certain extent to heed data already being acquired. Target companies that have crucial non-compliance issues, such as deriving data from illegal or non-compliant sources or non-compliant data processing could bring acquirers off-road, which essentially nobody wants. It could be understandable considering the following cases.

The Hacked Hotel case shows us why it is needed to check cybersecurity issues before M&A process. This hotel's reservation system was hacked. Two years later, Group Naive,

which is a large international group, acquired the respective hotel, even though it did not cover or check the system vulnerabilities at any stage of the due diligence process. After a two years M&A process, this hack was discovered that more than 300 million respective personal data had been stolen. Later one year, the respective data protection authority imposed a fine amounting of 25 million dollars on Group Naive since not obeying the respective data protection rules. In addition Group Naive faced compensation suits from customers that infringed their privacy. According to this case, it could be said that if Group Naive, before M&A, had heeded data compliance due diligence, it would possibly have identified these insufficient protection systems, then managed the acquisition from that perspective. They would have put a bargain on this crucial problem in determining purchase price.

Another case is similarly regarding data stolen. Buyer that is Company Drenched completed an acquisition exceeding 200 million dollars with Rainy Clouds, which is a cloud-based multi-channel payment platform. Company Drenched noticed that hackers had stolen data including personal data and crucial financial data hardly one million users from Rainy Cloud's servers. Because of security concerns, Company Drenched suspended all of Rainy Cloud's operations a few months after the M & A process. Ultimately, it makes acquisition nonsense for Company Drenched.

One more example is regarding the event that the due diligence process accomplished very well. Manufacturer Flying High intended to acquire Manufacturer Too Low, that is aircraft components, for 650 million dollars. Nevertheless, parties had decided to reduce the proposed price to 420 million dollars due to the fact that Manufacturer Too Low's system faced malicious ransomware attack by hackers. Yet, when this attack shut down important operations, parties could not meet a suitable agreement.

A major telecom Group V detected data breach in the case acquisition process with multinational internet Group Y. Thus, final acquisition prices dropped approximately 350 million dollars. Even parties made an agreement sharing costs arising from data breach in addition expenses of investigations and compensations stemming from third party claims. All these cases illustrate to what extent cybersecurity or other data compliance issues can essentially affect the price of agreements or in some cases off-road deals. Even though previous examples shows that the reason why data diligence mechanisms is paramount for Buyers, as for seller's perspective, data diligence also is needed since they could attain better outcomes before detecting any infringement by buyers. It makes their company more value.

The important point is that it should not confuse the regular due diligence process with the data diligence process. Even though a regular due diligence process involves to some extent data diligence questions, unfortunately, it would be insufficient and has to be identified and overlooked. Generally, they do not heed a sensitive area or subject to scrutiny of all respective data.

### **1.3. Data Diligence Steps**

Data Diligence covers 3 essential and important aspects. First element is regarding compliance of data. Data collection, storage, processing, transmission, disclosure, using issues on the table. Second element is whether measurement is in place for cybersecurity or data compliance. Whether measures serve the purposes to hinder data being illegally stolen, leaked, transferred, abused, or destroyed? Third element is regarding any incident coming from a cyber-attack or personal data infringement. Is there any litigation, investigation or penalties at current or past?

When evaluating data diligence for a target company, some questions have to be raised for buyers' benefit. Buyers have to identify data according to respective regulations, then determine data which one is relevant to its respective business. For instance, if some data is sensitive, it needs a special covering process whether the target company complies with the respective regulations. When some data is not relevant to non-personal data, however, it needs to be identified in some cases on the expert's eye, since it could be identified trade-secret such as formula or having a value. In some situations, target companies could use part of critical infrastructure or relevant services. If so, it needs to evaluate the systems target company use whether they are vulnerable or having preventative measures. For instance, some companies uses cloud computing i.e. saving their data or SaaS or any other operating platforms including websites, mini programs.

As a result, when data is in our mouth, it has to be said that many respective regulations such as GDPR, Data Act, Cybersecurity Act, NIS Directive and so on. To understand better whether all these regulations are complied with by the targeted company. Buyers need any experts that could evaluate the target company's compliance. Unfortunately, some companies resist complying with all these fresh regulations or drafts, however, it has to be understood that after a certain time, these provisions would determine the company's values in the near future.

### **1.4. Liability Regime Considering Court Cases**

What would be a liability when due diligence processes leave on professionals? It has to be checked, even though this decision could undergo change otherwise. Case is regarding the acquisition process given by the District Court of Dusseldorf in Germany. Target company has made a collective employment agreement with "Tarifgemeinschaft Christliche Gewerkschaften für Zeitarbeit und Personalserviceagenturen" (CGZP). (Collective Bargaining Association of Christian Trade Unions for Temporary Employment and Personnel Service Agencies). After the M & A process, the German Federal

Employment Court rejected the respective collective agreement because of CGZP's bargaining capacity. It means that all collective employment agreements are deemed invalid. Acquired company had to face and bear social security payment obligations. Law firm that made the due diligence process on behalf of the acquirer company had not indicated potential risk of CGZP's bargaining capacity and associated risks. Nevertheless, the court rejected the law firm's liability since law firms' responsibility is merely regarding *deal breakers* i.e. conditions and risks that would be crucial for the prospective buyer's decision. In addition, when due diligence occurred, there had not yet existed any case law that could refer to lack of bargaining capacity. Even though some scholars point out that point, according to the case, it would not be a reason to load any responsibility because of abstract ground not concrete. Ultimately, according to the case, buying decisions would not have depended on this abstract discussion.

Therefore, Law firms get rid of responsibility. Even though another case is related to the property due diligence process given by the Court of Appeal Of Berlin, it has to point out since this court ascertained the contract made between the law firm and the acquirer company. This court also again gave a decision regarding not liability for lawyers since their tasks agreed with the company is not part of that potential risks. Because courts ascertain the agreement as a service agreement, thus, lawyers could not bear this risk they did not point out. In the event of defect performance of a service contract, according to German law, the company had to demand supplementary performance. If they do not, they could not directly demand compensation from lawyers due to lack of review. Even if this case is not relevant to the M & A process, it is important which contract terms have to be determined while evaluating the relationship between the law firm and the company. In my opinion, lawyers have to determine their task in a written way. Nevertheless, it has to be emphasized that lawyers always bear attention in order to hinder any liability due to lack of scanning of due diligence.

## **2. It security due diligence**

Every day, businesses face danger not just from hackers but also from their own employees. There are a growing number of unseen dangers associated with relying on third- and fourth-party providers, which are nevertheless an integral part of any successful business model.

For the purpose of cyber security and to limit their legal exposure in the event of a data breach, businesses are doing extensive due diligence evaluations of all of its connections, partners, and potential clients.

When it comes to M&A, cybersecurity due diligence is crucial because it allows discoverers to make educated decisions about cybersecurity and related responsibilities. This knowledge is also helpful in the realm of cyber insurance, where it may be used to construct a security risk rating score and plan for mitigating hazards.

### **2.1. The Need for Such a Due Diligence**

Every company, no matter where it is located, may benefit greatly from performing cybersecurity due diligence. Accurate risk assessment prior to liability assumption in mergers and acquisitions, as well as the identification of concerns that may need deal restructuring, are two of its many benefits. Additionally, it aids businesses in recognizing and responding to cyber threats. It's also possible to quantify and identify an employee's total cybersecurity posture.

Unfortunately, Even the Most Advanced Businesses Often Lack Adequate Planning. Target company has cutting-edge offerings, strong sales force, and frugal operations, all of which bode well for a successful merger or acquisition. However, investors should not rely just on self-disclosure when trying to assess cybersecurity risk.

Cybersecurity due diligence services are being used by private equity firms, hedge funds, investment banks, and venture capital investors all over the world to make more informed merger and acquisition choices.

You may rest easy knowing that the cybersecurity record and future of your target organization is solid with the help of independent cyber due diligence. If you want to prevent or properly account for potential risks, fines, and costly remediation after a transaction has closed, our specialists can assist you identify material cyber-related issues that must be remedied.

The risks and gaps in information security can be found in governance, operations, and technology.

Learn more about data breaches that haven't been made public.

Evaluate the target's preparedness to identify and deal with a cyberattack.

Investigate the possible operational, financial, and reputational costs of remediation based on known and unknown risks.

Cyber due diligence is performed in the context of mergers and acquisitions to identify potential threats that could have an effect on the parties involved. The danger landscape of businesses also varies significantly between sectors, just as do the types of cyber hazards that businesses face. This means that some potential acquisition prospects may call for more extensive due diligence than others.



Due diligence should be more extensive throughout the M&A lifecycle for acquisition targets that will play a larger role in your day-to-day operations. It's better to find and fix possible cybersecurity issues before closing a contract than to have them pop up later. Conducting due diligence in M&A deals also helps to create standards against which future investments can be evaluated. With this in place, the due diligence phase of potential future purchases is simplified. **Heading 2: Cyber due diligence in M&As**  
When analyzing a potential merger or acquisition target, it is essential to do cyber due diligence based on the level of risk involved. During the M&A process, you can take advantage of the three phases below to do thorough due diligence.

### *Data Inventory*

How much data an organization has, where it is housed, and how it is moved can all be learned from a data inventory or data map. Information security threats that your company may face after the deal closes might be better understood with the aid of a data map.

There is continued utility for data maps even after an M&A transaction has closed. In most acquisitions, the target company must make a sizable payment to the acquiring firm. Taking precautions to ensure a safe data transfer is essential for enterprises to prevent compliance issues. You can lessen the cyber risk related to data transfers if you do an inventory of the data involved before you seal the agreement. Using the data flow map, you can keep tabs on data's origins and implement safeguards to keep it safe while it's in transit.

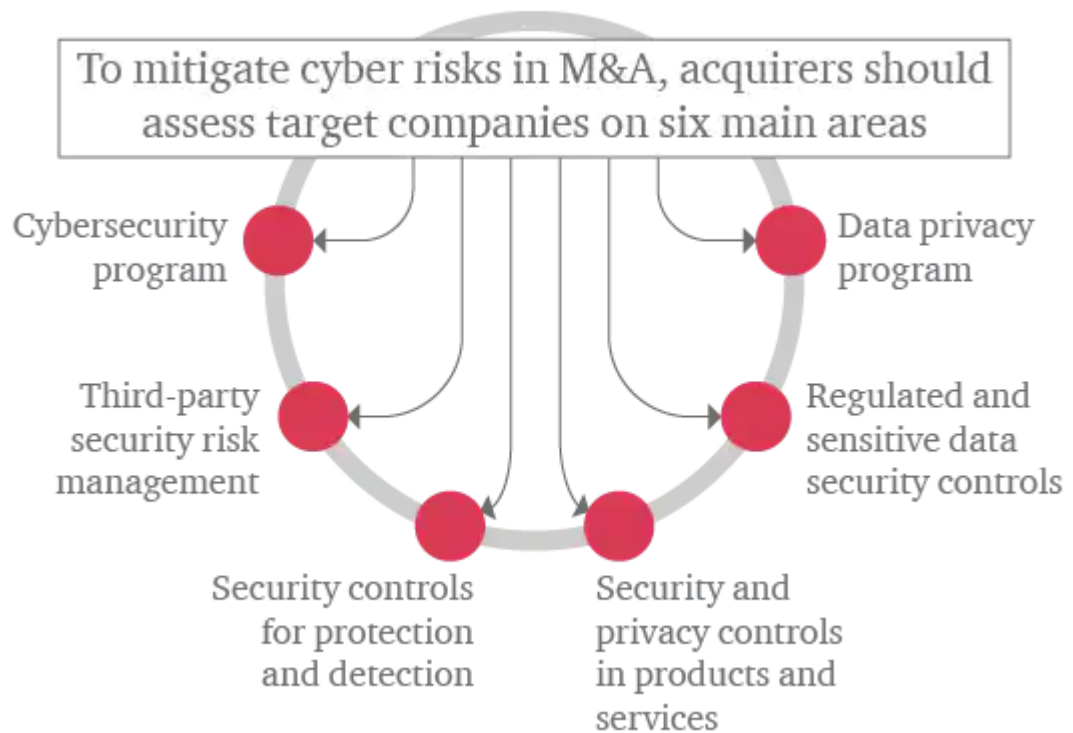
### *Review internal and External cybersecurity assessments*

A target organization's risk profile can be better understood by reviewing previous cybersecurity assessments. Be sure to request copies of any and all recent cybersecurity assessments, whether they were completed internally or by external auditors. These can also be used to judge how well an organization deals with threats. At the merger and acquisition (M&A) stage, be ready to ask the target company pointed questions about how it has used previous cybersecurity assessments to enhance its security operations. They should have some processes in place that track the efficacy of security controls, as this is an important part of cybersecurity evaluations.

### *Creating an integration strategy*

It is crucial to develop a plan for integrating the target company into the acquiring company before closing the purchase. When several network systems merge into one,

it can leave serious security holes that can be exploited for malicious purposes if proper protocols aren't in place. That's why hackers frequently hunt for weaknesses in freshly purchased businesses. Network compatibility testing is typically handled by the chief information officer or chief security officer, but if you don't have either of those people on staff, you can hire a vendor to conduct it for you.



Retrieved from:  
<https://www.pwc.com/us/en/services/consulting/deals/library/understanding-cyber-due-diligence.html>

## 2.2. Be Aware of Threats and Bad Actors

Before closing any agreements, acquirers should do cyber due diligence based on the level of risk involved. It was previously mentioned that cyber due diligence isn't as well-established as other sorts of due diligence and doesn't assess standardized data. The same level of due diligence is not necessary for every business because no two transactions are identical.

In order to protect the parties involved in a merger or acquisition, a buyer needs to have a system in place to assess the external and internal threats they face and to identify the bad actors who pose such threats. In addition, extra due diligence is warranted for higher-risk deals, including as purchases in high-insecurity nations or sectors that have recently been the target of attacks.

### **2.3. Frequency to Flexibility**

Companies that engage in a high volume of transactions, such as private equity or serial acquirers, should incorporate cyber at every stage of the deal life cycle. Those that often engage in mergers and acquisitions should have a cyber deals playbook that can be adjusted to accommodate each stage of the deal process, any level of cyber risk, and any type of deal. This helps acquirers better manage cyber risk to targets and their existing portfolio by incorporating cybersecurity at critical times in the deal life cycle.

Managing cyber risk in transactions also results in establishing a baseline of cyber readiness that can be utilized across the company's portfolio and in evaluating potential new investments. Some investors will test the safety of their portfolio firms once a year in order to better position them for future acquisitions.

### **2.4. Identification and Quantification**

The acquirer's cyber due diligence should also identify deal-breakers or, at the very least, deal-changers. Although it's quite uncommon that a customer will walk away entirely, there could be problems that cause them to reevaluate the target's worth. An acquirer needs to be able to quantify these concerns and either require the target to fix them prior to closure or renegotiate the price and other terms.

The latter may present a chance to redirect purchase price to seller-funded remediation investment, but the acquiring company still requires a strategy for dealing with and paying for the problem after the deal closes and during the integration process. However, serial acquirers who are confident in their ability to manage the risks of smaller purchases may find the possibility of shifting the burden to sellers appealing.

Cyber due diligence's end result should be a prioritized list of remedial tasks, complete with who's responsible for them, how much it'll cost, and when it'll be done.

### **2.5. European Cyber Security Certifications EUCS**

ENISA has introduced new legislation on cybersecurity certification in order to increase confidence in cloud services across Europe. The primary objective of the program is to improve and standardize the cyber security of cloud services within the European Union's internal market. To guarantee that cloud service protections meet EU and worldwide standards, a candidate system for EU Cloud Services has been developed.

According to the ENISA proposal, "the purpose of these additional standards is to appropriately avoid and limit the possible interference by governments outside the EU with the functioning of authorized cloud services." Although this again exhibits the direct characteristics of data localization, it has been met with pushback from several member states like the Netherlands, Ireland, and Sweden due to sovereignty limits on European data localisation and foreign law. Implementing and auditing sovereignty requirements will be cumbersome, time-consuming, and costly, all while reducing competition and driving up prices.

With the recently enacted revision of the Network and Information Security directive (NIS2 Directive, COM/2020/823), businesses that provide vital services will be required to implement the program's highest degree of assurance. According to the draft, the high assurance technique will make it impossible for businesses located outside of Europe to obtain the certificate due to territorial limits. The cloud service provider must have European headquarters, cannot be operated by a non-EU entity, and must not be subject to non-EU law. The proposed European Union Cybersecurity Certification Scheme for Cloud Services (EUCS) and the Trust and Labeling Framework of the Gaia-X Association both include requirements for "immunity" from the laws of third nations.

## **2.6. GAIAX Sovereign Cloud**

Among the many initiatives included in the European Commission's (EC) 2020 European data plan is the creation of a federated cloud, often known as a sovereign cloud for Europe. This is the first official EU policy on data localization, if it exists at all. The Von der Leyen commission, a leader in data strategy, has advocated for substantial investment in the advancement of such projects to ensure Europe's technological and cloud sovereignty. The approach emphasizes the European Union's (EU) minuscule share in the cloud market and its reliance on third-party suppliers. This endangers the privacy and security of European data, so the continent is focusing on developing a sovereign cloud service that is not reliant on third-party service providers.

Though first conceived as a direct challenge to Europe's excessive reliance on American cloud services, GAIA-X has morphed into an initiative to bring the area together. However, it is not yet obvious what function the hyperscalers will play in the consortium despite their participation. If the project is reorganized and focused, however, it has the potential to evolve into a privacy-PaaS layer compatible with all major cloud hyperscalers. Users can continue to make use of either the providers' infrastructure services or their preferred platform offerings, depending on the configuration. Therefore, we may utilize the technical advantages, elasticity, and scalability of the hyperscalers while also elucidating the data concerns. Thus, GAIA-X would become a globally relevant technology, not simply in Europe. In this approach, GAIA-X can be used to monitor actual compliance with these internationally endorsed standards.

### **3. Data Privacy And M&A Transactions**

#### **3.1. The Relation Between GDPR and M&A Transactions**

The EU's General Data Protection Regulation ("*GDPR*") has been becoming a crucial factor in mergers and acquisition ("*M&A*") transactions by adding complexity to the due diligence process. The GDPR regulates both criminal and civil sanctions in case of data breaches during M&A transactions as well as increases enforcement action by regulators. Therefore, the companies might possibly encounter higher fines and the risk of reputational damage to both sides, buyer and target company. Regardless of acting either as buyer or seller, companies shall be aware of the volume of the transferred data throughout the M&A transactions at each stage. To be compliant with data privacy rules, mainly GDPR, it is key to take into consideration data protection requirements as early as possible. Alongside being compliant from the beginning, companies should ensure the necessary documentation whether they are well-prepared in order to mitigate the risk of liability once the data incident occurs.

Considering the effect of GDPR on M&A transaction, in fact, more than half (54%) of respondents had worked on M&A transactions that had not progressed because of concerns around a target company's data protection and compliance with GDPR, according to a recent survey of 500+ M&A practitioners across Europe, the Middle East and Africa (EMEA) by Euromoney Thought Leadership Consulting. [1] GDPR has wide applicable broad, since all the organizations which collect or use personal data are bound by data protection requirements. It can be clearly said, most target companies are highly likely to share the data they have from their employees, suppliers or customers as examples. Thus, acquiring parties shall be cautious in order to avoid GDPR exposure. With the lack of appropriate measures and recognition of risks during M&A transactions in a sense of data protection, data breach incidents might become apparent solely after a deal has already been concluded which in fact results in expensive exposure and potential litigations.

#### **3.2. Handling with Data throughout M&A Transactions**

The GDPR applies as long as the purchasing or selling company is based in the European Union. In the meantime, due to its extraterritorial effect, the GDPR must also be taken into consideration in corporate transactions in which the merging companies are based outside the EU. The GDPR regulates on the concept of accountability, and imposes demonstrable processes, controls and proactive oversight of data processing activities which also cover the context of mergers, acquisitions, investment and funding rounds.

In recent times innovative businesses are more and more frequently dependent on information technologies and accordingly data processing. The more innovations, the more revenue as long as compliance and effective cyber security strategy is held in case of data breaches and high fines.

In the preliminary stages of any M&A transaction, widely speaking, parties shall extend the data protection statements to envelope the transfer of personal data to third parties with the context of assets, restructuring, merger or sale by means of "extension of declaration of purpose". Moreover, parties shall make sure that the proper documentation regarding data transfer such as "data processing agreements" are in place.

The due diligence process throughout M&A would be greatly contributed once the target company has data protection compliance mechanisms properly and is able to demonstrate them in accordance with the accountability principle. Since at that point, it must be also taken into account that personal data might flow between different parties which are third countries, in other words outside of the European Economic Area. As a result, both parties of M&A transactions must ensure that they are compliant with data protection requirements for the international transfers before finalizing the deal. Data transfer safeguards which stem from GDPR steps once the data will be transferred to third parties. Data transfer safeguards vary, and must be used accordingly to the need whether adequacy decisions or standard contractual clauses would be sufficient. Therefore, in this work, recommended steps to handle data are examined as follows.

### **3.3. Non-Disclosure Agreements and Confidentiality**

Especially in the early stages of M&A transactions, the buyer and target company shall determine whether either one of them has been faced with GDPR fines before. At the end of the day, M&A transactions surely cover data sharing considering data of employees, customers, suppliers, vendors, and/ or clients and so on and so forth on a global scale. This means a confidentiality agreement and a non-disclosure agreement shall be in place properly in order to have sufficient documentation once the personal data is shared. Confidentiality by means of NDAs thus plays an active role to prevent data sharing without legitimate interest.

Considering measures stemming from GDPR, once the personal data is shared for some reason, parties shall have a virtual data room in which only necessary staff has access. The virtual room must be reached with limitations as well as monitoring rights so as to prevent misuse of the data. Such industries have to be even more diligent due to the fact that they might have special data known as sensitive data[1], in order to run their business; e.g. hospitals, and banks. Adherence to the data minimization principle that stems from GDPR is essential. The target company should only upload personal data that

is explicitly relevant and necessary for the purposes of assessing the asset and settle any redundant data. Special category personal data with respect to employees can be broad, such as their racial, ethnic origin, political opinions, or health data which are subject to robust controls under the GDPR. Thus, it is vital to take additional measures by limiting any of this data with enhanced access controls. It must be noted that none of the lawful bases which are given by GDPR for processing data are not applicable to special categories of data in the context of an M&A transaction. In other words, companies should avoid uploading or disclosing any special category data as part of the M&A process, unless it is anonymized, thus, it no longer identifies the data subjects.

### **3.4. The Storage of Shared Data**

The storage of data can be either virtual or physical, yet the fundamental requirements do not vary. The diligently created space for the data can be a secure cloud which saves important documents and files for an M&A transaction. Parties have to ensure who is being granted access to this server under which terms and conditions. In particular, buyers should restrict the distribution of personal data; on the other hand, the target company shall follow a privacy policy which regulates potential data sharing in case of M&A transaction. It is advantageous to use data rooms for due diligence, hence virtual data rooms provide a high level of security, easy file management as well as activity tracking and analyzing.

### **3.5. Accountability**

Both sides of the M&A transaction are obliged to stipulate the lawful basis for the data processing; they shall examine the data protection issues before the term sheet is signed. The buyer would in fact ask for warranties from the target company so as to make sure that there will be legitimate sharing of data due to M&A transactions. With the help of this check, the buyer is able to be sure there is not any unauthorized processing of data. This responsibility covers which data has been shared at any time of the transaction, for what reasons, with who, etc. so as to prove compliance.

It should be mentioned that the target company may possibly have an agreement with its data subjects regarding the data transfers to third parties. If it is the case, the data owner has already consented to the data sharing, thus, accountability here will be an easier task for the processing among the target and buyer of the M&A deal.

However, it has to be emphasized that companies should not fully rely on consent since the consent from the employee might not fulfill the requirements of “freely given consent”. So to say, consent would not be a lawful basis to disclose employees' personal data. Since valid and appropriate consent is only possible as long as it is freely given as the European Data Protection Board accepts. The validity of the consent therefore can

be doubted considering the employment context due to the imbalance of power. Eventually, the employee is not highly likely to have genuine control over his data.

### **3.6. Warranties**

As said in this work, data breaches incident may result in considerable fines, thus, the buyer shall make an effort to require the seller to give warranties, especially confirming, *inter alia*. It makes sense to list some examples regarding warranties;

The target business has not had any data security breach incidents in its history, or not engaged in a dispute over a data protection offense; is well equipped with adequate IT and cyber security mechanisms; is diligently and regularly audited for its IT and cyber security compliance; has well-structured data protection policy.

Moreover, the buyer should require indemnification by the seller for any breach of these warranties, as well as for any mistake to comply with data protection law, since they may have arisen prior to the M&A if it is commercially possible. On the seller's side, despite the fact that in principle any liability that may be created when the seller performs the control of the target should be taken by the seller. Although the sellers shall also clarify the limit of its liability, whether in terms of amount, duration, and/or nature of damages.



## Bibliography

Emily Liner, "What 's the behind Allt Time High in M&A", Retrieved from, <https://corpgov.law.harvard.edu/2016/03/16/whats-behind-the-all-time-high-in-ma/#:~:text=They%20may%20be%20interested%20in,processes%2C%20property%2C%20or%20personnel> on 17.10.2022

Limitations of lawyers' professional liability for legal due diligence, Retrieved from <https://www.gvw.com/en/news/blog/detail/limitations-of-lawyers-professional-liability-for-legal-due-diligence> 09.10.2022

Mark Schaub , Zhao Xinhua , Wang Zhefeng , Tan Qiyao and Shan Wenyu, DUE DILIGENCE ON DATA IN CHINA INVESTMENT AND M&A PROJECTS, retrieved from ,<https://www.kwm.com/cn/en/insights/latest-thinking/due-diligence-on-data-in-china-investment-and-ma-projects.html>, on 01.10.2022

Why M&A needs data due diligence, retrieved from <https://legaldw.com/latest/why-m-a-needs-data-due-diligence>, on 01.09.2022 WILLIAM J. GOLE, PAUL J. HILGER, Due Diligence an M&A Value Creation Approach, Wiley Publishing, 2009

James Waddell, "Data Protection Issues on Due Diligence and Disclosure", Retrieved from <https://www.stevens-bolton.com/site/insights/briefing-notes/data-protection-issues-on-due-diligence-and-disclosure> on 13.10.2022

Kison Patel, "What is a Due Diligence Virtual Data Room?", Retrieved from <https://dealroom.net/blog/what-is-a-due-diligence-virtual-data-room> on 13.10.2022

Katie Knowles, Alexander R. Roth, Dr. Paul Voigt and Wiebke Reuter, "Data privacy in M&A Transactions", Retrieved from <https://www.lexology.com/library/detail.aspx?g=4c766594-f1dd-46c8-8b96-1347833d75d7> on 14.10.2022

Carolyn Bigg, Joe Bauerschmidt and Teerin Vanikieti, "Impact of Data Protection Laws on Mergers and Acquisitions (M&A) Transactions", Retrieved from <https://www.dlapiper.com/en/thailand/insights/publications/2019/09/impact-of-data-protection-laws-on-mergers-and-acquisitions-mna-transactions/> on 15.10.2022

<https://www.pwc.com/us/en/services/consulting/deals/library/understanding-cyber-due-diligence.html>

<https://www.cloudflare.com/en/blog/why-gaia-x-hasnt-been-successful-yet/>

<https://www.forrester.com/what-it-means/ep289-future-of-gaiax/>

<https://www.euractiv.com/section/digital/opinion/gaia-x-a-trojan-horse-for-big-tech-in-europe/>

<https://medium.com/infobipdev/could-gaiax-save-european-digital-sovereignty-607f6f6294d3>

+ + +




*M&A Transactions, Due Diligence in IT  
Security, Data, and Data Protection*

*Legal Lab, Herfurth & Partners*

*Mustafa Enes Balin  
Irem Atik  
S J Jagannadh Palepu*

1



## Data Due Diligence

- General Framework
  - Data Due Diligence
  - When Due Diligence on The Table
  - What is Data Diligence
  - Data Diligence Steps
  - Liability Regime Considering Court Cases

2



## Data Diligence

-Many companies tend to try merger and acquisition process in order for their growth to increase due to the fact that other growth component is insufficient to extend their volume

-M&A process could be accomplished two ways: strategic or financial.

On the strategic level, companies could cut costs by combining process, property or personnel.

On the financial level, it is led by a group of investors, such as private equity companies, which is a type of alternative investment in which the investors purchase shares in privately-held business.

3



## When Due Diligence On The Table

-Acquirer could only have general familiarity, not could reach a crucial data regarding targeted company.

- This situation makes acquirer depend on merely assumptions which could bring naturally failure.

- Due diligence is a important tools in order to prevent such failures by looking closely.

Ultimately, acquirer gain comfort that a target company is what it is represented to be in addition validates key assumptions and mitigates the risk that acquisition will bring bring unwelcome surprises

4



## What is Data Diligence

- With the advance of Big Data, a new manner has emerged around data analyses during M&A. To understand better, basically hardly every company is directly related, greater or lesser extent, somehow data.

It also affect surely M&A process.

- After that point, M&A process has driven in a certain extent to heed data already being acquired. Target companies that crucial non-compliance issues, such as deriving data from illegal or non-compliant sources or non-compliant data processing could bring acquirer off-road, which essentially nobody wants.
- Showing some cases

5



## Data Diligence Steps

- Data Diligence covers 3 essential and important aspects.
- First element is regarding compliance of data. Data collection, storage, processing, transmission, disclosure, using issues on the table.
- Second element is whether measurement is in place to cybersecurity or data compliance. Whether measures serve the purposes to hinder data being illegally stolen, leaked, transferred, abused, or destroyed?
- Third element is regarding any incident coming from cyber attack or personal data infringement. Is there any litigation, investigation or penalties at current or past?

6



## **Liability Regime Considering Court Cases**

- District Court of Dusseldorf- collective employment agreement
- Court of Appeal Of Berlin- written requirements of lease agreement

7



## **DATA PRIVACY AND M&A TRANSACTIONS**

8

### **The relation between GDRP and M&A transactions**

- EU's General Data Protection Regulation ("**GDPR**") has been becoming a crucial factor in mergers and acquisition ("**M&A**") transactions by adding complexity to the due diligence process.
- Therefore, the companies might possibly encounter higher fines and the risk of reputational damage to both sides, buyer and target company.
- To be compliant with data privacy rules, mainly GDPR, it is key to take into consideration data protection requirements as early as possible.
- Companies should ensure the necessary documentation whether they are well-prepared in order to mitigate the risk of liability once the data incident occurs.

9

- Considering the effect of GDPR on M&A transaction, in fact, more than half (54%) of respondents had worked on M&A transactions that had not progressed because of concerns around a target company's data protection and compliance with GDPR, according to a recent survey of 500+ M&A practitioners across Europe, the Middle East and Africa (EMEA) by Euromoney Thought Leadership Consulting.
- With the lack of appropriate measures and recognition of risks during M&A transactions in a sense of data protection, data breach incidents might become apparent solely after a deal already has been concluded which in fact results expensive exposure and potential litigations.


10



### **Handling with Data throughout M&A Transactions**

- The GDPR applies as long as the purchasing or selling company is based in the European Union. In the meantime, due to its extraterritorial effect, the GDPR must also be taken into consideration in corporate transactions in which the merging companies are based outside the EU.
- In recent times innovative businesses are more and more frequently dependent on information technologies and accordingly data processing. The more innovations, the more revenue as long as compliance and effective cyber security strategy is held in case of data breaches and high fines.

11

- 
- Parties shall extend the data protection statements to envelope the transfer of personal data to third parties with the context of assets, restructuring, merger or sale by means of "extension of declaration of purpose".
  - Moreover, parties shall make sure that the proper documentation regarding data transfer such as "data processing agreements" are in place.
  - It must be also taken into account that personal data might flow between different parties which are third countries, in other words outside of the European Economic Area. As a result, both parties of M&A transactions must ensure that they are compliant with data protection requirements for the international transfers before to finalize the deal.
  - Data transfer safeguards vary, and must be used accordingly to the need whether adequacy decisions or standard contractual clauses would be sufficient.

12

### Non-Disclosure Agreements and Confidentiality

- Especially in the early stages of M&A transaction, the buyer and target company shall determine whether either one of them has been faced with GDPR fines before.
- A confidentiality agreement and a non-disclosure agreement shall be in place properly in order to have sufficient documentation once the personal data is shared.
- Parties shall have a virtual data room in which only necessary staff has access. The virtual room must be reached with limitations as well as monitoring rights so as to prevent misuse of the data.
- Adherence to the data minimization principle that stems from GDPR is essential. The target company should only upload personal data that is explicitly relevant and necessary for the purposes of assessing the asset and settle anonymize any redundant data.

13

### The Storage of Shared Data

- The diligently created space for the data can be a secure cloud which saves important documents and files for an M&A transaction.
- In particular, buyer should restrict the distribution of personal data; on the other side, target company shall follow a privacy policy which regulates potential data sharing in case of M&A transaction.
- It is advantageous to use data rooms for due diligence, hence virtual data rooms provide high level of security, easy file management as well as activity tracking and analysing.

14



### Accountability

- Both sides of the M&A transaction are obliged to stipulate the lawful basis for the data processing, they shall examine the data protection issues before the term sheet is signed.
- It should be mentioned that the target company may possibly have an agreement with its data subjects regarding the data transfers to third parties. If it is the case, the data owner has already consented to the data sharing, thus, accountability here will be an easier task for the processing among the target and buyer of the M&A deal.
- However, it has to be emphasized that companies should not fully rely on consent since the consent from the employee might not fulfil the requirements of “freely given consent”.
- Appropriate consent is only possible as long as it is freely given as European Data Protection Board accepts.

15

### Warranties

- Data breaches incident may result in considerable fines.
- Ideally, the target business;

has not had any data security breach incidents in its history, or not engaged in a dispute over a data protection offense.

is well equipped with adequate IT and cyber security mechanisms.

is diligently and regularly audited for its IT and cyber security compliance.

has well-structured data protection policy.

16



## IT SECURITY DUE DILIGENCE

*"IF YOU SPEND MORE ON COFFEE THAN ON IT SECURITY, YOU WILL BE HACKED. WHAT'S MORE, YOU DESERVED TO BE HACKED!"*

Cybersecurity incidents

Cyber Incident

Understanding Cyber due diligence with risks and a toolkit!

17

## An Unprecedented Look at Stuxnet, the World's First Digital Weapon

### Court Approves Class Action Settlement in RE: YAHOO! Inc. Customer Data Security Breach Litigation and Guidelines to Future Class Action Settlements

Monday, August 3, 2020

Yahoo!'s data breach class action is finally being put to rest. Last month, the Northern District of California approved the proposed **\$117.5M** settlement to resolve the claims of approximately 194 million class members in *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2020 U.S. Dist. LEXIS 129939 (N.D. Cal. July 22, 2020). This approval did not come easily. During several rounds before the Court to obtain settlement approval, the Court pointed out that while "other data breach cases focus on one data breach, the instant case involves *multiple* data breaches over a period of five years, each of which Yahoo failed to timely disclose."

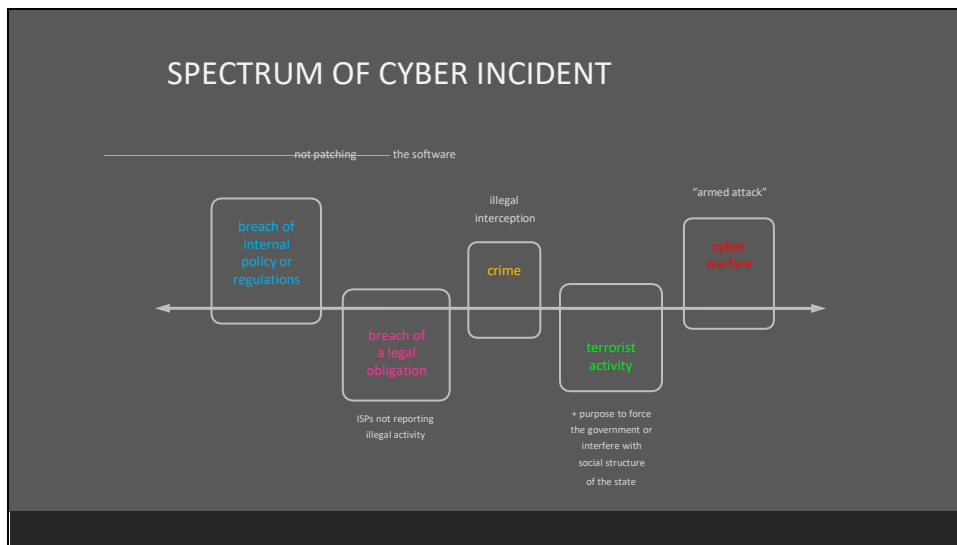


18



# Wannacr y (2017) Ransomware Crypnoworm

19



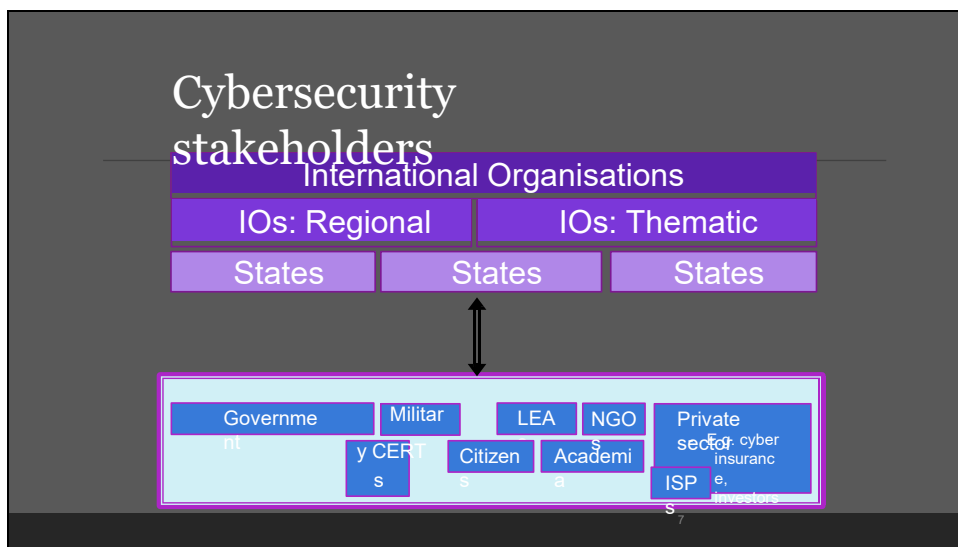
20

### What Are the 50 Most Common Passwords

Based on most common duplicate passwords within a breach of over 30 million accounts

1. 123456	11. 123321	21. 222222
2. 123456789	12. 1q2w3e4r5t	22. 112233
3. qwerty	13. iloveyou	23. abc123
4. password	14. 1234	24. 999999
5. 1234567	15. 666666	25. 777777
6. 12345678	16. 654321	26. qwerty123
7. 12345	17. 555555	27. qwertyuiop
8. 1234567890	18. gfhjkm	28. 888888
9. 111111	19. 777777	29. princess
10. 123123	20. 1q2w3e4r	30. 1qaz2wsx

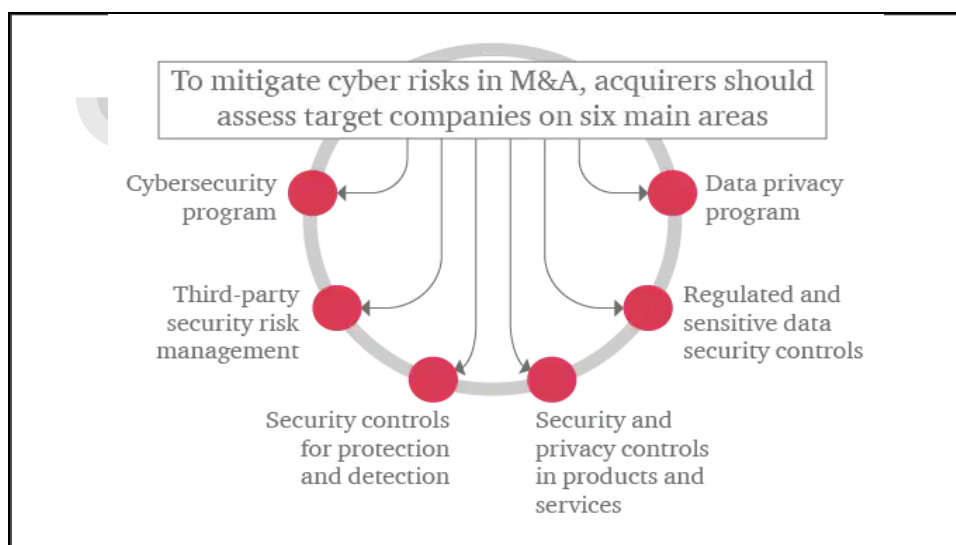
21



22



23



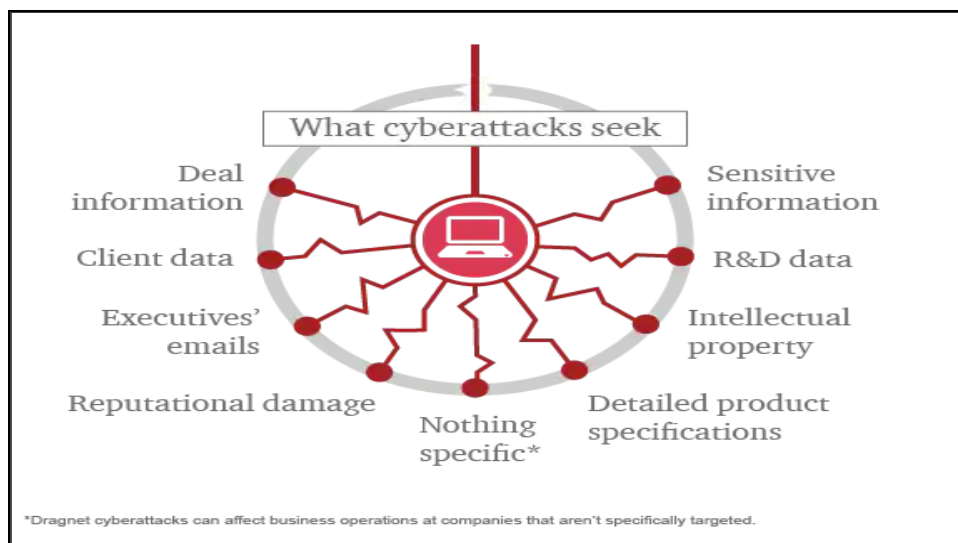
24

Instead of relying solely on data provided by an M&A target, analyzing information available from *outside the target is becoming increasingly valuable* to understanding risks.



The diagram illustrates the concept of analyzing information from outside the target. It features a central building icon representing the target. To its right is a large red plus sign. Further right is a vertical stack of icons, each enclosed in a rounded rectangle. From top to bottom, these icons are: a pie chart, a clipboard with a checkmark, a document, a bank building, a plus sign, a laptop with a person icon, a plus sign, a smartphone, a plus sign, a bank building, and a bar chart. This stack represents various external data sources that can be analyzed to understand risks.

25



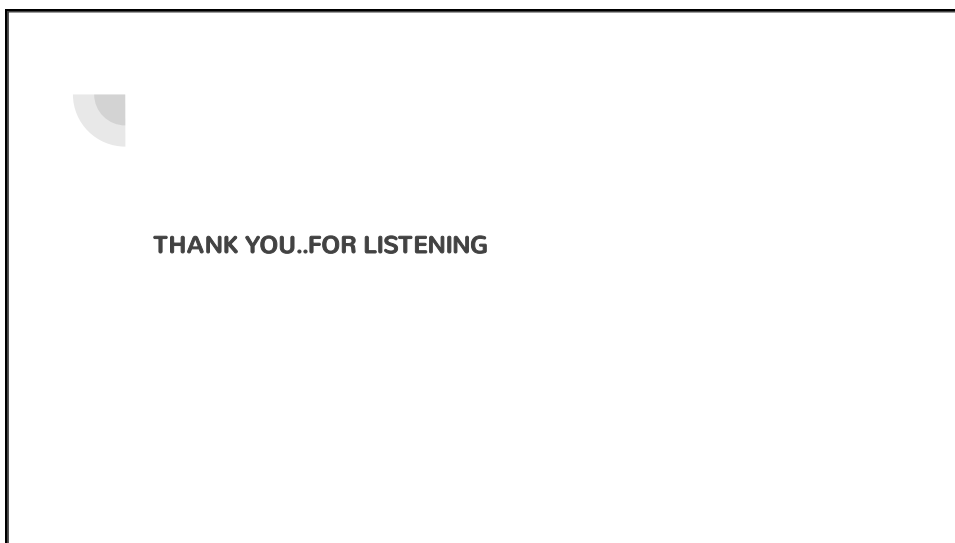
26

- Many companies permit their employees to use personal mobile devices to access company-specific information.
- Key Areas of Diligence:
  - What is the scope of the company's control of the employee's mobile device?
  - To what extent does/can the company monitor the employee's use of the mobile device?
  - Are there procedures in place to restrict the transfer of data from the mobile device?
  - Does the company use a Mobile Device Management (MDM) application? Such as:
    - Airwach
    - Soti
    - Xen Mobile
    - Microsoft InTune
  - Can the data on the mobile device be remotely wiped? By Whom?
  - How are lost devices managed?

27

- **Shared User Accounts**
  - Sometimes companies create a shared username and password to allow several employees to log into a single workstation or application.
- **Unmanaged Backups**
  - It's essential to mix remote backups with onsite backups, and it's imperative that a trained professional monitor backup alerts.
  - What is your backup policy?
- **Sensitive Information Sent Over Email**
  - Generally the contents of email passing through the internet is insecure.
  - The best secure encryption solutions apply filters to automatically encrypt messages containing confidential information.

28



29