Deloitte.

A call for Heroes in the Jungle of Data Laws

Roles and responsibilities in the application of European data and AI regulations

MAKING AN IMPACT THAT MATTERS since 1845

Foreword

In response to the growing importance of the data economy, the EU is issuing several laws and draft legislation as part of the EU Data Strategy. This regulatory framework includes GDPR, the law protecting personal data which came into effect in May 2018, as well as more recent laws, such as the Digital Services Act and the Digital Markets Act, which both took effect in November 2022, and draft legislation for the Data Act and the AI Act, which we expect to be adopted in 2024. To apply these new laws in practice as efficiently and effectively as possible, the key first step for most companies is to define the required roles and responsibilities. This Point of View gives you structured guidance on how to select the right people to champion compliance within your organization, first considering which departments would be eligible and then using a scorecard approach based on different decision criteria to determine the most suitable candidates for the project as well as the key considerations in each case.

The data economy and data legislation in the EU

"The only constant in life is change". These wise words of Greek philosopher Heraclitus still very much apply today. Today's companies are under pressure to adapt at ever shorter intervals not only in terms of technological advances but also the regulatory environment.

Unlike many other technologies from electromobility to 3D printing, digital trends and data-driven innovations are unique in that they affect MANY or even ALL areas of an organization. They offer a wide range of opportunities in R&D, production, sales and other core operations of a company, but the complexity of applying the associated data-related regulations in practice can be quite a challenge.

With the recent introduction of the EU's General Data Protection Regulation (GDPR), companies have had to learn the hard way how challenging this can be.

And now there are even more EU regulations on the way as part of the EU Data Strategy, which, according to the Commission, is designed to create "a genuine single market for data and make Europe a global leader in the data-agile economy."[1] One such law, which is already in effect, is the Digital Services Act, but the EU has also recently published draft legislation for the forthcoming Data Act and the AI Act.

Tab. 1 – Overview of important EU data strategy laws

Important European laws or draft laws as part of the EU data strategy	Aim of the law	Status
General Data Protection Regulation (GDPR)	Protects personal data	In effect since 2018
Regulation on the free flow of non-personal data	Ensures organizations can store and process non-personal data anywhere in the EU	In effect since 2019
Digital Markets Act	Establishes rules for digital gatekeepers and protects against abuses of market power	In effect since 2022, in part applicable as of 2022, and in part as of 2023
Digital Services Act	Protects consumers in the digital environment	In effect since 2022, in part applicable as of 2023, in part as of 2024
Data Governance Act	Provide the framework for fostering collaborative use of data	In effect since 2022, applicable as of 2023
AI Act	Protects against the risks of Artificial Intelligence (AI)	Planned for 2023
Data Act	Promoting fair and transparent data	Planned for 2024

[1] Data Act Proposal, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0068, accessed 06/20/2023.

The difficult path to compliance with new data-related laws

Of course, the industry is not exactly idle. The Data Act and the AI Act are already under intense discussion in many companies, with expert reports being prepared and risks for various departments being highlighted. There are also numerous articles and posts on social media analyzing individual aspects of the draft legislation. And yet, very few companies seem to have launched coordinated initiatives or strategies for their actual application. To put it provocatively: a lot of talk, but very little action. Awareness about the new laws seems to be growing in many companies, but actual initiatives have been lacking.

The date these regulations come into force is fast approaching, and if the industry's experience with GDPR has taught us anything, we know it can take months or even several years – as well as enterprise-wide effort – to comply with the requirements of a new law as comprehensive as the Data Act. So, what is holding these companies back?

The Bystander Experiment of Latané and Darley

Attracting a lot of media attention in the 1970s, this experiment involved sending test participants to a waiting room where smoke suddenly began to spread through the crack in the door. If the participant was alone in the waiting room, he or she usually got up immediately and left the room to get help. However, if the participant was in the room with several people who did nothing (because they were actors who were in on the experiment), he or she usually hesitated for ten or up to 20 minutes before actually addressing the obvious issue and trying to escape.

Even though everyone is aware of what needs to be done, no one takes action because of this group dynamic. If no one is officially "appointed" to act, lead and decide, nothing gets done – not even when the negative consequences are clearly visible.

This effect is also well known in the fairy tale genre, by the way, as seen in Hans-Christian Andersen's "The Emperor's New Clothes".

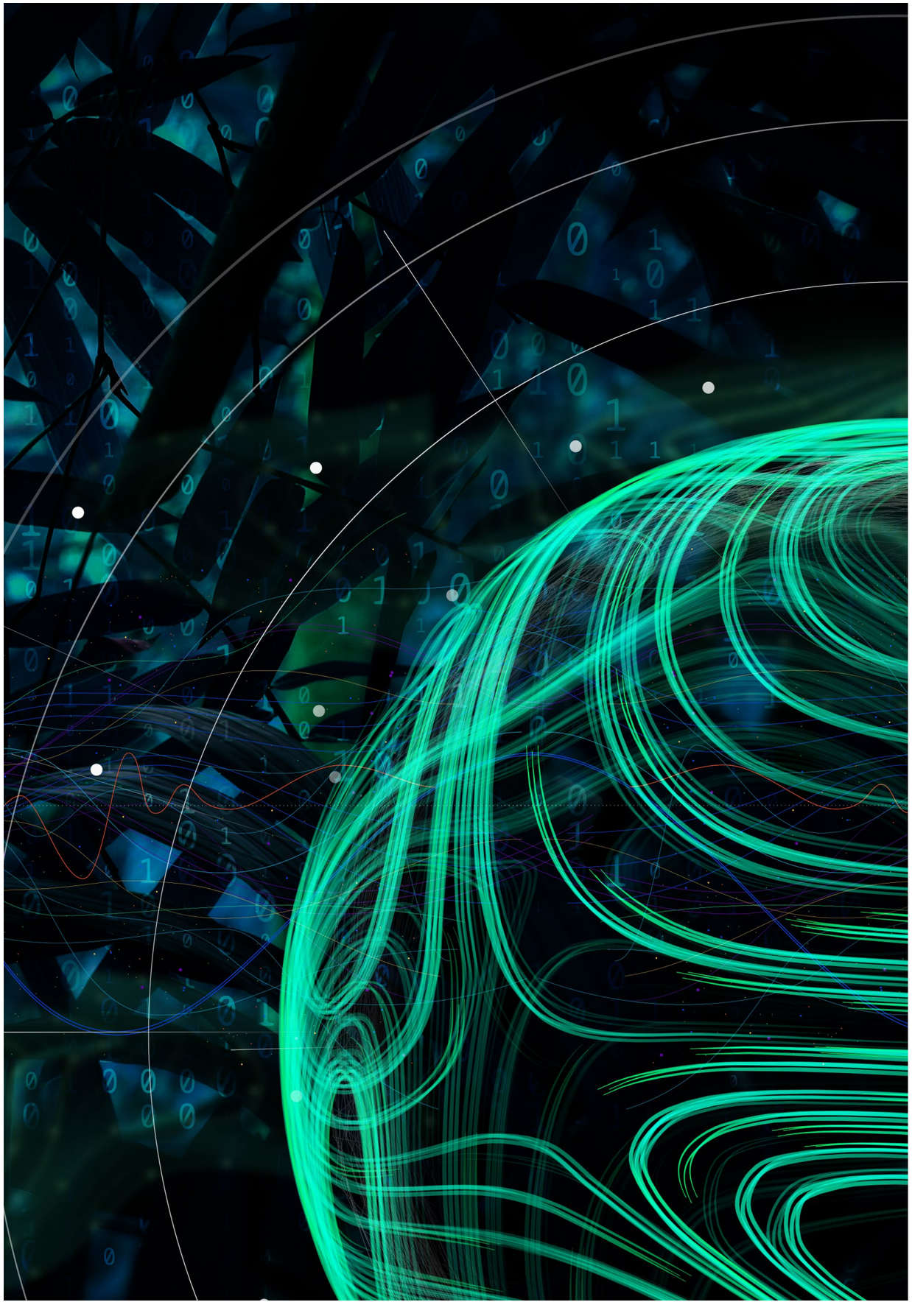
What the Bystander Experiment can teach us

We believe that companies will not be able to adopt an effective and efficient approach to complying with data-related legislation until they appoint a specific role for the project. Up to that point, the best intentions of any number of people across the organization will remain just that – intentions – with potentially dramatic adverse effects enterprise-wide.

In behavioral psychology, experts use the phrase "diffusion of responsibility" to describe this phenomenon, i.e., not performing a task that obviously has to be done, even though there are plenty of capable people available to do it. The higher the number of actors involved, the less the individual recognizes his or her subjective responsibility and the less likely it is that any one individual will take action. This is sometimes also referred to as "pluralistic ignorance".

So, everyone knows what needs to be done, and is quite capable of doing it, but refrains from taking action as long as no one has an official mandate. The famous Bystander Experiment cited here is a prime example of the diffusion of responsibility.

To avoid diffusion of responsibility, management would ideally designate a specific role for any new area of responsibility as quickly as possible. This means in more concrete terms that management must appoint a responsible person or department for all the compliance issues that arise – e.g., from the Data Act – in good time. It will be this person's responsibility to introduce the necessary steps, and he or she will need sufficient resources and the authority to do so. Moving forward, management will receive regular reports on the progress of application measures and their ability to reduce compliance risk for the company as a whole.



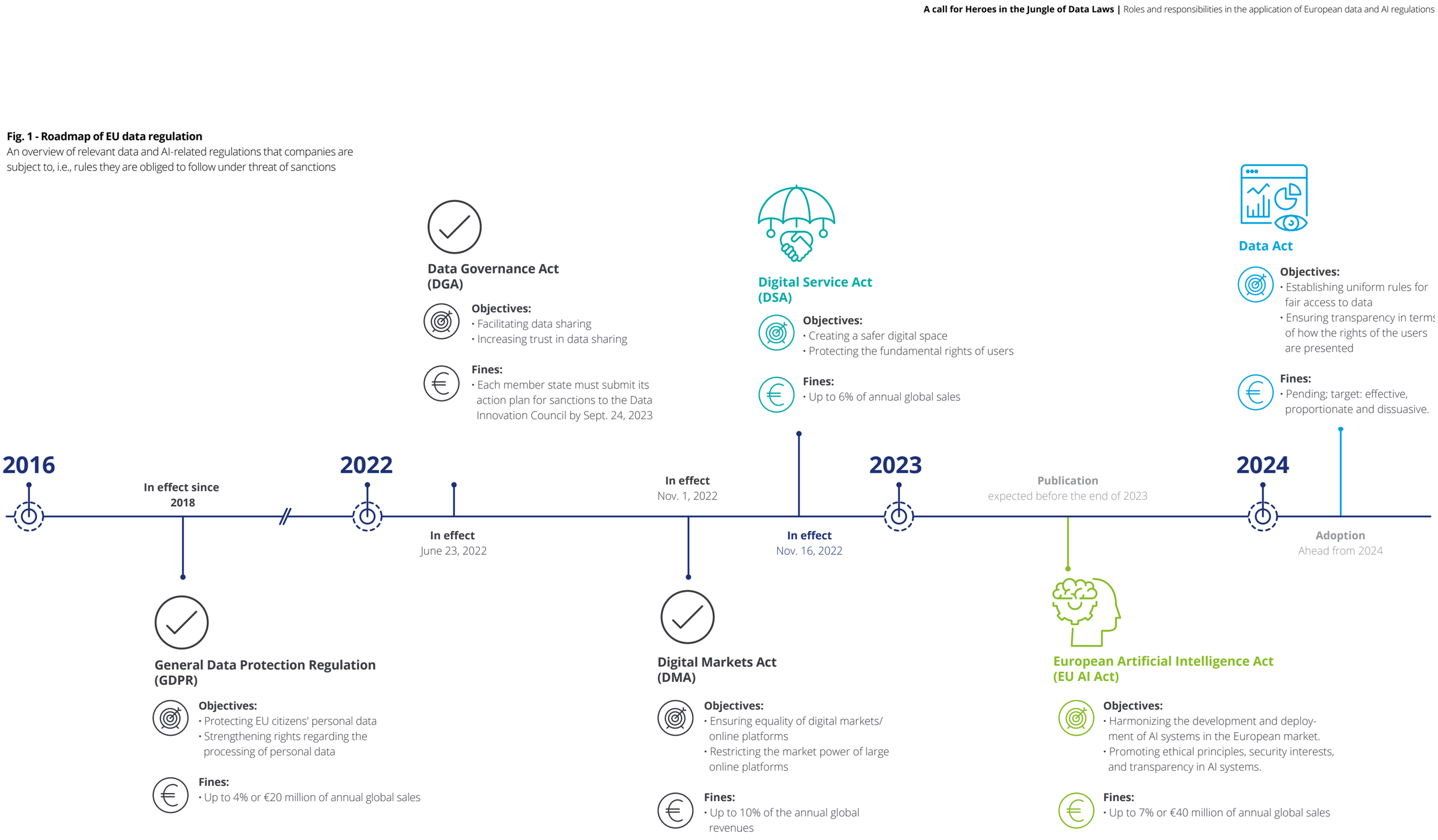
Laws and implications of the EU data strategy

Today, data is the cornerstone of the digital world and an essential building block in the value creation chain. Data is collected and processed in many places, which creates a wide range of opportunities for the companies that collect the data to utilize or exploit it.

The European Commission has recognized this as both a potential and a threat. To keep pace with the ongoing digitalization and technology advances, the EU has launched a number of initiatives and additional laws as part of its broader data strategy (see Fig. 1).

Over the next few years, virtually all companies will be affected by legislation under the EU Data Strategy.

Fig. 1 - Roadmap of EU data regulation
An overview of relevant data and AI-related regulations that companies are subject to, i.e., rules they are obliged to follow under threat of sanctions



For this Point of View, we are focusing on the Digital Services Act (which is already in effect and, unlike the Digital Markets Act, is relevant to many companies), as well as the Data Act and the AI Act (both of which have not yet been adopted but will have a huge impact on companies across all sectors).

Responsibilities for applying data-related laws in companies

In our observation, companies still have a great deal of uncertainty as to which departments are best suited to implement the requirements of the various laws.

In contrast to data protection law (GDPR), these other laws do not explicitly name a specific role with fixed responsibilities. For example, Art. 37 and 38 GDPR describe the role of the data protection officer and his or her tasks, required skills and responsibilities. In the Data Act, AI Act and Digital Services Act, by contrast, no such role is discussion.

The EU Commission has also not yet named the supervisory authorities that will be responsible for enforcing the three laws mentioned here. This information would be helpful, because once the companies know which authorities they will be communicating with, it might provide some indication about the unit best suited to the project.

As it stands, each company will have to decide for itself which department within the organization is the right choice.

Our goal in this Point of View is to provide some guidance by identifying, analyzing and evaluating various key criteria for the three laws mentioned above. We have created a matrix and side-web graphs (see Fig. below) to visualize the results. You can easily combine them with other criteria that apply specifically to your company, which will help you find the right department for you.

Establishing the right roles and responsibilities is a critical success factor for any company when it comes to applying new laws in practice.

Potential departments to consider

Though every company has its own organizational structure, there are certain departments that are frequently under discussion for application of the laws in question. They are as follows:

- **Legal department**
- **Antitrust/Competition officer/ department**
- **Consumer Protection officer/department**
- **Risk Management**
- **Chief Compliance officer/ department**
- **Data Protection Officer/ department**
- **Chief Data Officer/ department**
- **CISO/ IT Security**
- **CIO/IT department**
- **The specialist department with most use cases**
- **A newly created department**

Not every company has all the departments mentioned here. If that is the case in in your company, not all of those listed above will be an option, unless there is a department that assumes one of these roles.

Identifying the suitable accountability – methodology and evaluation criteria

1. Affected by scope

Here, we consider the extent to which a particular department is directly affected by the law and its provisions. For example, the department that operates an online retailer's e commerce site is directly affected by many of the requirements of the Digital Services Act and is obliged to comply with them on its platform. A legal department is not directly affected by these requirements, even if it can serve as an advisor.

2. Content proximity/ skill synergies

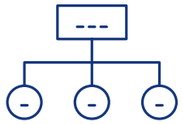
This criterion has to do with the existing expertise a department has that might be thematically related to the expertise required to apply the new law. Risk management, for example, already has a great deal of knowledge about the requirements of the AI Act, whereas the CISO department probably does not.

3. Structural proximity/ process synergies

We use this criterion to assess whether a company can harness existing processes and practical experience from similar projects for the new law and use company resources more efficiently. Many elements of the Data Act, for example those concerning the contractual obligations of data transfer, are closely related to data protection. As a result, the data protection department may have a higher score here than the antitrust department.

4. Capacity/budget/ equipment available for the project

Here, we are not suggesting that the existing staff or budget allocation has sufficient scope to apply the new laws in practice. After all, each of these laws requires a large-scale, organized effort, much like other major projects. It is more relevant here, for example, if a department already has experience with similar types of projects and would therefore be more aware of the policies and procedures needed to acquire the necessary funding – on an interim or a permanent basis. Legal departments are not generally familiar with these kinds of projects, whereas the CDO or his/her department often does.



5. Suitable organizational alignment

We use, among other things, the three-lines model here (see Fig. 2). This model will be relevant during the application of all three laws and subsequent operations for two reasons: the project can be extremely complex from a technological standpoint, and the potential losses in the event of a violation can be substantial. As a result, second-line departments within the organization receive a higher score here than their first-line counterparts or those that are "on the sidelines".

6. Suitable reporting line/ no conflict of interest

This final criterion is also related to governance and the three-lines model. Due to the significant impact of potential non-compliance with these laws (fines, reputation, etc.), it makes sense to have a direct reporting line to the management/board of directors wherever possible. It is also important here to determine whether there is a conflict of interest between the department's functional mandate on the one hand and the tasks potentially required to apply the law in practice on the other. For example, the IT department will face such a conflict if its job is to source the most cost-efficient and user-friendly IT applications possible, but also to implement the (possibly cumbersome and costly) requirements of the three laws.

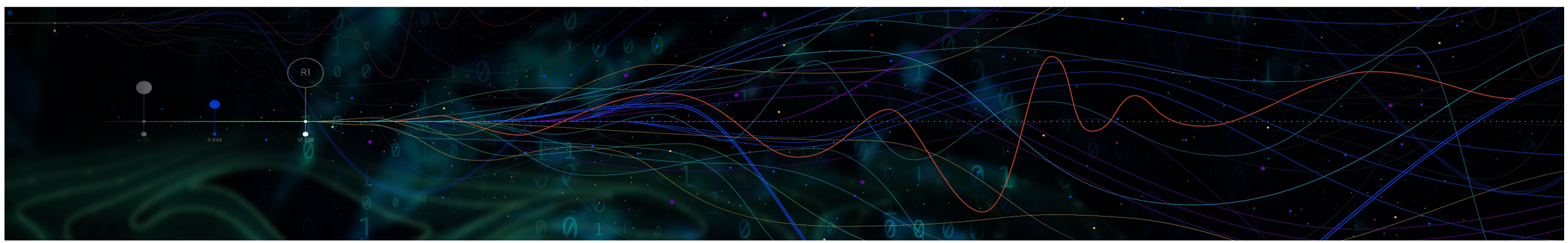
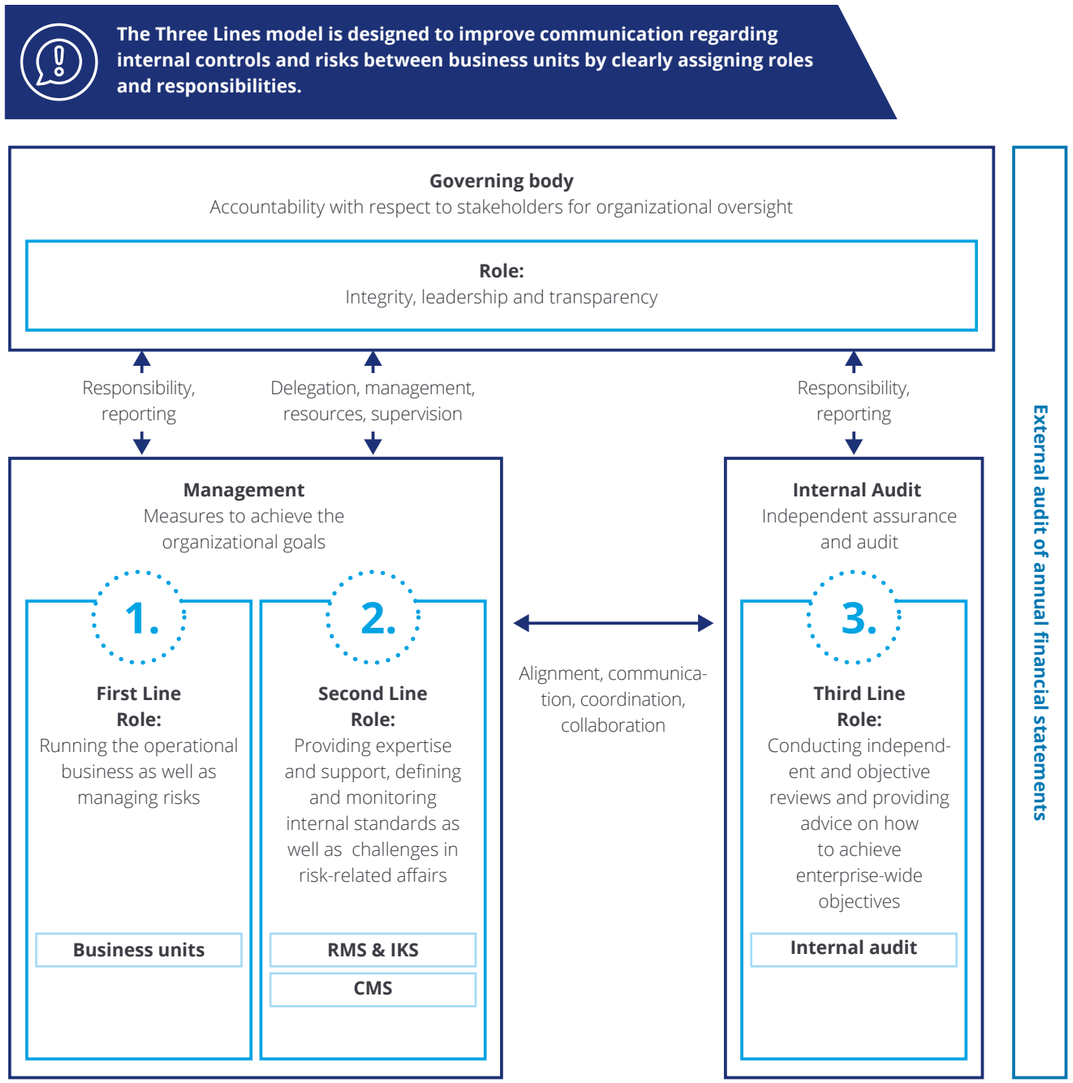


Fig. 2 – Three Lines Model



Hinweis: Angelehnt an IIA: Three Lines Modell (2020), s. 2 f. (veröffentlicht im Juli 2020 als aktualisiertes Modell des zuvor bekannten „Three Lines of Defense" Models)

The following table shows the results of our evaluation as a scorecard. The higher the score, the more suitable a department is for implementing the requirements of a particular law. The matrix is as follows:

1 = little to no applicability
2 = proportional applicability
3 = (mostly) applicable

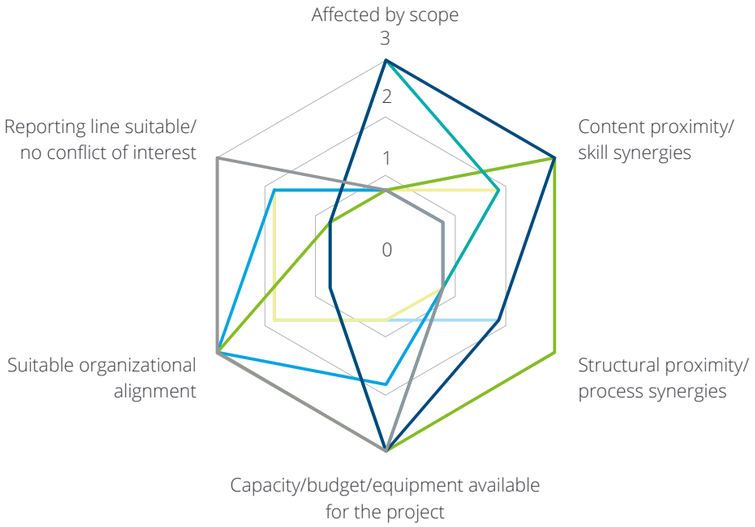
Tab. 2 – Scorecards: Digital Service Act, Data Act & AI Act

Scorecards: Digital Services Act, Data Act & AI Act								
Role \ Factor		Affected by application scope	Content proximity/ skill synergies	Structural proximity/ process synergies	Capacity/ budget equipment available for the project	Suitable organizational alignment	Suitable reporting line/no conflict of interest	Total
	Legal department	**1**, **1**, **1**	**2**, **2**, **2**	**1**, **1**, **1**	**1**, **1**, **1**	**2**, **2**, **2**	**2**, **2**, **2**	**9**, **9**, **9**
	Department for antitrust law/ competition law	**1**, **1**, **1**	**1**, **2**, **1**	**1**, **1**, **1**	**1**, **1**, **1**	**2**, **2**, **2**	**2**, **2**, **2**	**8**, **9**, **8**
	Department for consumer protection	**1**, **1**, **1**	**3**, **2**, **1**	**2**, **1**, **2**	**1**, **1**, **1**	**2**, **2**, **2**	**2**, **2**, **2**	**11**, **9**, **9**
	Risk Management	**1**, **1**, **2**	**2**, **1**, **2**	**1**, **1**, **1**	**1**, **1**, **1**	**2**, **2**, **2**	**2**, **2**, **2**	**9**, **8**, **10**
	Chief Compliance Officer/Compliance department	**1**, **1**, **1**	**1**, **1**, **1**	**1**, **1**, **1**	**2**, **2**, **2**	**3**, **3**, **3**	**2**, **2**, **2**	**10**, **10**, **10**
	Data security officer/data security department	**1**, **1**, **1**	**3**, **3**, **2**	**3**, **3**, **3**	**3**, **3**, **3**	**3**, **3**, **3**	**3**, **3**, **3**	**16**, **16**, **15**
	Chief Data Officer/CDO department	**1**, **2**, **1**	**3**, **3**, **3**	**3**, **3**, **3**	**3**, **3**, **3**	**3**, **3**, **3**	**1**, **1**, **1**	**14**, **15**, **14**
	CISO/IT-Security	**1**, **1**, **1**	**1**, **1**, **1**	**1**, **1**, **1**	**3**, **3**, **3**	**3**, **3**, **3**	**3**, **3**, **3**	**12**, **12**, **12**
	CIO department	**3**, **3**, **2**	**2**, **2**, **2**	**1**, **1**, **1**	**3**, **3**, **3**	**1**, **1**, **1**	**1**, **1**, **1**	**11**, **11**, **10**
	Department with the most use cases	**3**, **3**, **3**	**3**, **3**, **3**	**2**, **2**, **2**	**3**, **3**, **3**	**1**, **1**, **1**	**1**, **1**, **1**	**13**, **13**, **13**
	Newly created department	**1**, **1**, **1**	**1**, **1**, **1**	**1**, **1**, **1**	**3**, **3**, **3**	**3**, **3**, **3**	**3**, **3**, **3**	**12**, **12**, **12**

Summarizing the results of the scorecard, we get a similar picture for all three laws. The larger the shape for the individual roles, the better the respective role/department is suited to application of a law. The figures show a general picture, related to the selected evaluation criteria. Of course, as these can also vary from company to company, your result may rely on different priorities.

The graphs give a basic overview of how the regulations of the EU Data Strategy are applied. They show that the standards set by the EU Data Strategy follow a similar pattern.

Fig. 3 - Digital Services Act



The picture is similar for all the three laws.

Fig. 4 - Data Act

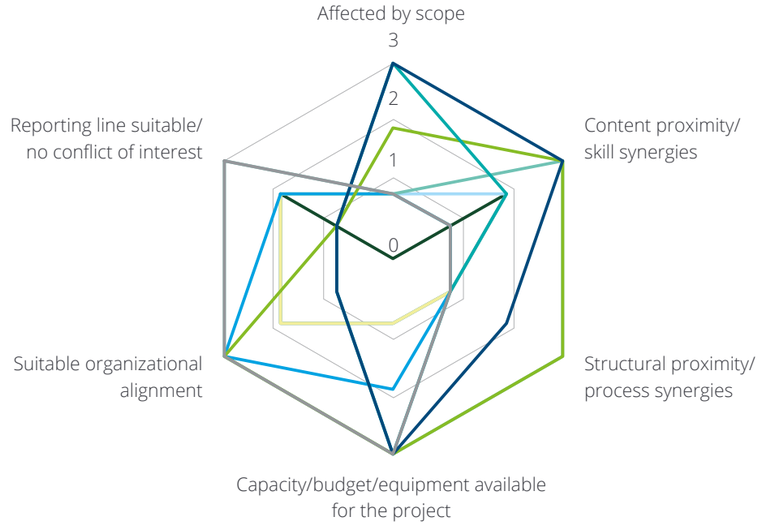
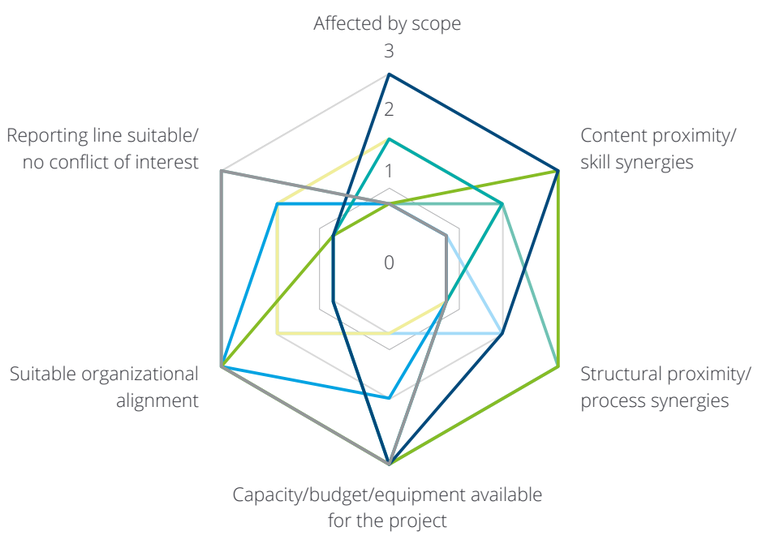


Fig. 5 - AI Act



- Legal department
- Department for antitrust law/competition law
- Department for consumer protection
- Risk Management
- Compliance Officer – Compliance department
- Data security office – Data security department
- Chief Data Officer/CDO department
- CISO/IT-Security
- CIO department
- Newly created department
- Department with the most use cases

Identifying the suitable accountability – Explanation of the results

We get a similar picture for all three laws, with only slightly different scores.

Legal departments or similarly structured departments (e.g., labor law) are less suitable for this project, even though these departments may have more legal expertise with regard to projects such as these. This is mainly because these departments are not set up to carry out large-scale projects or to serve in a classic second-line role.

Units that are directly affected by the laws (i.e., primarily the respective specialist departments and the IT department) only score in the middle range in the overall assessment. This is primarily due to the results for governance criteria 5 and 6.

Staff units within the GRC – i.e., Compliance, Risk Management as well as, in an extended sense, the CISO department – also end up in the middle range. Although compliance is one of their core competencies, they usually lack expertise in data-related procedures, structural elements and processes.

Setting up a completely new, made-to-measure department to implement the requirements of these laws sounds tempting at first. After all, you could build every structural element required for the project on what amounts to a “greenfield site". However, this idea does not have the top score, because it fails to take advantage of a great many opportunities for synergies with existing elements within the company. This makes implementation not only time-consuming and expensive, but there is also a risk of friction loss in the day-to-day work with other departments closely focused on processes.

For all three laws, the CDO or his/her department and the Data Protection officer or his/her department receive the highest score, with the latter leading by a slight margin in each case. Both of these departments have all the advantages of their responsibilities for organizing data within the company, albeit with a slightly different focus. As a result, they naturally have a lot of skills in data handling already as well as the corresponding processes in place. Both departments usually have a good size staff and experience in large-scale projects: the CDO department more in terms of data governance, the Data Protection department more in terms of GDPR.

The main difference between these departments, which ultimately gives the data protection department its higher score, is the focus on data organization and, consequently, the reporting lines. While the CDO department is responsible for the data economy, the data protection department is tasked with protecting specific data owners – namely natural persons in their role as employees, customers, interested parties or service providers. That puts it clearly in the second line, with measures to help management avoid violating the law. For this reason, the Data Privacy department has no conflict of interest in reporting on the organization’s compliance regarding any of the data-related laws.

It is this organizational factor that gives the Data Protection department the edge in our ranking for all three data-related laws, i.e., the Digital Services Act, the Data Act and the AI Act. We should note once again that, from our point of view, this top ranking applies not only to personal data, but also to non-personal data. The main reason for is the huge synergy potential in the processes of the data protection management system for the application of the new laws in practice.

A good example here is the requirement for a notification system, which you need for both GDPR and the Digital Services Act.

Even if our scorecard analysis provides a clear result, there may be other aspects that play a role in your company’s decision-making process. Special employee configurations, capacity bottlenecks, individual mandates of certain departments or the absence of certain departments, specific requirements of the group and more might produce a different result for your company. You should, of course, take these aspects into account when making your decision.

In our experience, the following additional recommendations have proven helpful when deciding on the right department.

Legal department
If you decide to make your Legal department responsible for complying with the Digital Services Act, the Data Act and the AI Act, you can be sure that they will provide a solid analysis and in-depth description of the new legal environment in a legally confident manner based on your company’s specific circumstances. They will quickly identify any potential legal obstacles and draft legally-sound guidelines. The department will also be able to provide advice on individual issues, as it does in other legal questions.

However, it is important not to lose sight of the organizational, process-related and technical aspects of the project. Since Legal departments rarely have much experience with these aspects, we recommend bringing roles from other departments (e.g., IT, specialist departments) on board throughout the project in this scenario and/or relying on their own project management resources. These roles can assume responsibility for the design of processes as well as roles and draft the communication and training documents. Project management, status tracking and reporting deserve special attention and may be best assigned to PMO resources.

Finally, it is important to make a timely decision as to who will be responsible for the newly created processes and tools (possibly in the form of a separate management system) and who will continue to update them on a regular basis. If the Legal department also assumes the responsibility for line operations once the project is completed, it is vital to ensure they have the personnel with the right skill profiles for this in the medium term.

Antitrust/Competition officer/ department, or the Consumer protection officer/department
All the statements made for the Legal department apply equally to the Antitrust/ Competition or Consumer Protection officers/departments, as these have a similar set-up to the Legal department.

Some departments are only suitable for implementing the requirements of the EU Data Strategy under special circumstances.

Risk Management department
Particularly for the AI Act, which deals specifically with risk assessment, this department may seem like the obvious choice.

However, if your company decides to do go in this direction, we recommend working in close coordination with IT, the CDO, the specialist business departments and the Data Protection department throughout the project. It will be useful to give all these actors an opportunity to participate in the process of applying the new laws and, by the same token, to have a realistic idea of the personnel required so that this department is equipped to handle the project.

Chief Compliance officer/ Compliance department
In our experience, Compliance departments operate either solely in an overarching, framework-oriented role or deal additionally with such topics as money laundering prevention, anti-corruption and possibly also ESG. Data protection is usually not part of the compliance mandate but rather a separate area of responsibility. As a result, compliance departments generally do not have as much knowledge about data protection-related laws and the processes required.

If your company decides to put the Compliance department in charge of implementing the requirements of the Digital Services Act, the Data Act and the AI Act, we recommend that it coordinates very closely with the Data Protection department and the CDO, providing information on existing roles, processes and tools in the context of data protection and data governance. This will help to avoid duplication of work and costs.

You should also establish structures to avoid conflicts of interest in project reporting and line operations. To give an illustrative example here: Companies can use AI applications to significantly improve money laundering prevention. At the same time, the department in question will be required to report on the progress of the project, even though the application of the AI Act should avoid risks for natural persons wherever possible. If the same department is responsible for both mandates, it must take both factors into account, resulting in a conflict of interest.

CISO/IT-Security-department
Although ensuring compliance with data-related laws is not a typical responsibility for the CISO, we are aware of some companies considering putting the CISO in charge of applying the AI Act in practice. There are also some companies considering this strategy for the Data Act as well, especially if the CISO's department is responsible for data governance tasks.

If your company decides to go this route, we strongly recommend you have sufficient legal expertise for the project, which is usually lacking in the (IT-related) CISO department. It is essential, given the high penalties associated with these three laws, to carefully evaluate the various provisions of the laws – particularly as there are no lawyers in the CISO department in most cases.

CIO/IT department or the department with the most use cases
When it comes to implementing the requirements of these laws, IT and certain other departments have the advantage that they are directly affected by these laws, have first-hand knowledge of the use cases likely to arise in day-to-day operations and understand which application measures can be used in practice. This puts them in a classic first-line role. It is vital to rely on this valuable practical experience throughout the project regardless of the department you ultimately select.

If your company decides to put one of these departments in charge of implementing the requirements of the Digital Services Act, the Data Act and the AI Act, it will conflict with the three lines model from a compliance perspective, as these first-line departments are unable to audit themselves. In this case, we recommend working with the Compliance department to come up with a suitable structure for monitoring compliance with these laws.

As mentioned earlier, you also need to make sure there is sufficient personnel with the right skill profiles available. These roles will have to take responsibility for process and tool ownership (in the form of a separate management system where necessary) and be able to continue developing the system moving forward.

Newly created department

If your company has good reasons to put a new department in charge of applying the three laws in practice, we recommend close collaboration with all other roles mentioned in this Point of View to educate them about all the processes, roles and tools already in place.

The enormous coordination effort this requires in practice, especially in the initial period, raises concerns that it will inevitably lead to duplication of effort. Even more so, as each individual process should also be designed to ensure that no extra effort is required for interfaces to other processes. In terms of tool support, you should make every effort to use existing tools, e.g., from data protection management, to access the additional functionality you need rather than developing completely new tools.

Chief Data officer/CDO department

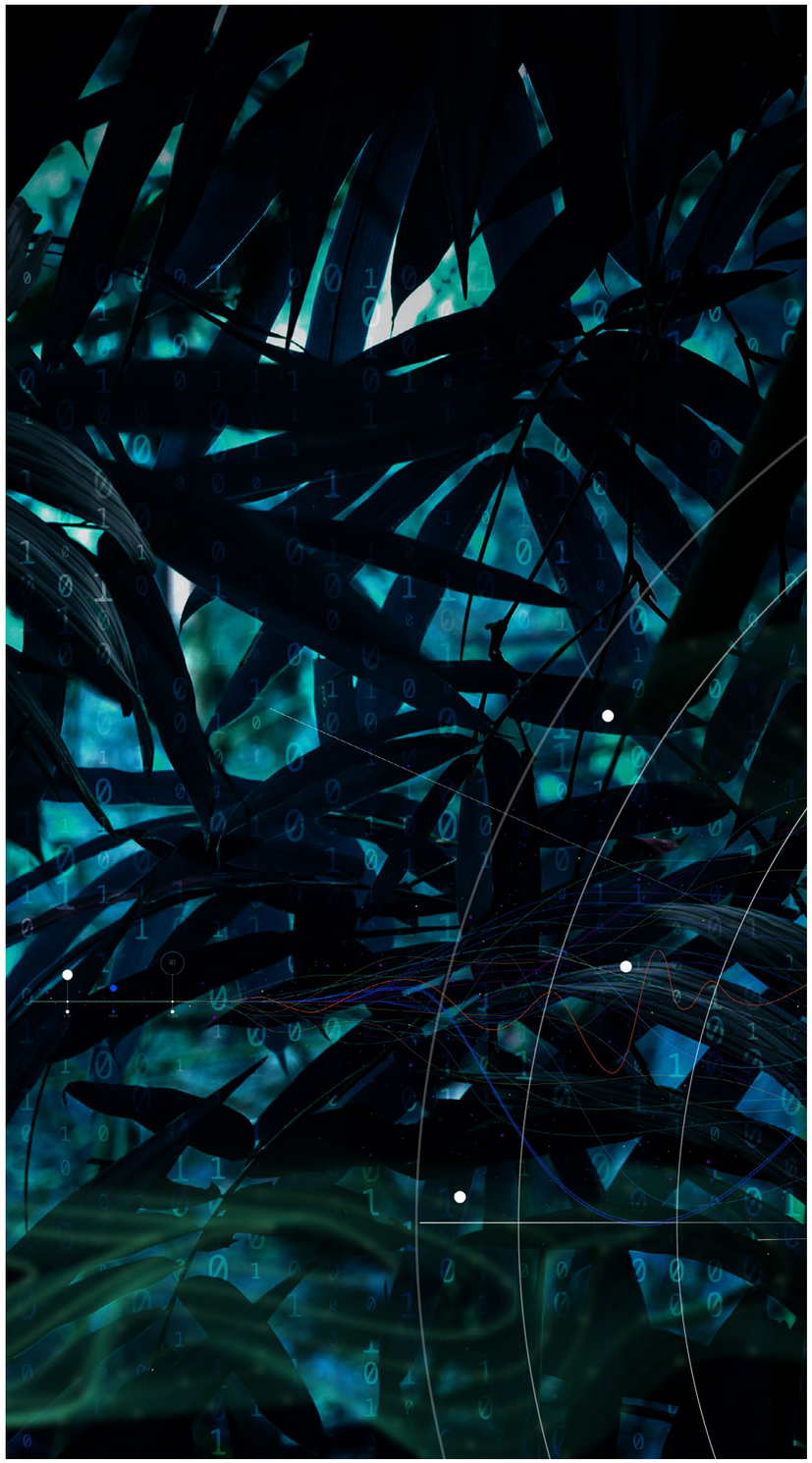
As is evident on the scorecards, we believe the CDO department is ideally suited to implement the requirements of the new data-related legislation.

While the CIO is usually in charge of the company's IT infrastructure and the technical side of data processing, the CDO manages data as an asset designed to maximize data-related value creation. This makes the CDO a key driver in the company's digital transformation and the content home of the data economy.

We can assume that the CDO department has sufficient experience in organizing and managing data to be able to assess the requirements of the Digital Services Act, the Data Act and the AI Act. Consequently, they will be able to apply them in the corporate context in a meaningful way, with the priority on financial results.

If your company decides to put the CDO department in charge of the project, however, you need to ensure it is grounded in sufficient legal expertise and makes a reliable assessment of the various legal implications.

It is also crucial to address and avoid any conflicts of interest with other tasks of the CDO department (e.g., maximizing data utilization) by structuring the project accordingly.



Data Protection officer/ Data Protection department

The Data Protection department has long-standing experience with GDPR's rules for handling personal data and can harness this experience in projects designed to apply other data-related laws in practice. The department has the tools and the processes it needs to manage data regulations and has already been established within the company as the central point of contact for data protection issues.

In terms of content, some of the structures put in place to manage data protection will also be useful for the Data Act. Under both the GDPR and the Data Act, for example, companies must comply with certain disclosure obligations to their users. Companies are also subject to contractual requirements under both laws (commissioned data processing for GDPR, contracts with users for the transfer of data to third parties). The way processing operations are documented under the GDPR (processing directory) may also be useful for the Data Act, as well as the parallels between the two laws in terms of data exchange and interoperability.

The data sets generated and used in practice often contain a mixture of personal and non-personal data that is difficult to separate. Expanding the department's data privacy management system into an end-to-end data management system that encompasses both types of data will help to prevent organizational inconsistencies and friction losses.

Another advantage to putting the Data Protection department in charge of applying the Data Act in practice is its experience in dealing with supervisory authorities. Since the rules on fines in the Data Act are strongly based on those in the GDPR, this experience could prove quite helpful. Art. 3(2)(a) of the Data Act explicitly states that the data protection supervisory authority is also responsible for the Data Act insofar as personal data is concerned.

If the Data Protection department is ultimately selected to drive application of the Digital Services Act, the Data Act, and the AI Act, we recommend incorporating the data analysis expertise of the CDO department or the technical expertise of the CIO department to put the project on a stronger foundation and to coordinate with the specialist departments regarding practical application and the feasibility of new processes.

You should also keep in mind that these new laws affect more than just personal data, that those in charge do not focus on personal data due to their history, and that the broader scope of the Data Act should be duly recognized. Finally, as with all other departments, it will be vital to increase staff accordingly to rise to the challenge of implementing the requirements of these laws in a timely manner.

Conclusion

Regardless of which department your company ultimately decide is best suited to apply these laws in practice, you should make the decision as soon as possible - after in-depth consideration of all relevant factors, of course. This is particularly important for the Digital Services Act (if not immediately for the Data Act and AI Act) and those companies that are subject to it, as it was adopted in November 2022 and will be in fully effect as of February 2024. That leaves precious little time for implementation.

To return to the Bystander Experiment: Don't wait until the room is full of smoke and you can no longer find a way out. The time is now to make the first and most important decision for implementing the requirements of these new data laws by appointing the right person or department for the job.

Your Deloitte contacts

Dr. Ljuba Kerschhofer-Wallner
Partner Risk Advisory
German Lead for Strategy,
Brand & Reputation
Tel: +49 89 29036 8329
lkerschhoferWallner@deloitte.de

Atrak Yadegari
Director Risk Advisory
Strategy, Brand & Reputation
Tel: +49 22 19732 4521
ayadegari@deloitte.de

Philipp Zimmer
Director Risk Advisory
Strategy, Brand & Reputation
Tel: +49 21 18772 5364
pzimmer@deloitte.de

Deloitte.

Issue 08/2023