This project is funded by the European Union.

TÜRKİYE AND EU
FINANCIAL COOPERATION
FUNDAMENTAL RIGHTS

Technical Assistance for Strengthening Fundamental Rights Sector Coordination

COMPARATIVE STUDY ON DIGITAL RIGHTS

(GERMANY-AUSTRIA-IRELAND)

CFCU
CENTRAL FINANCE & CONTRACTS UNIT

WEglobal

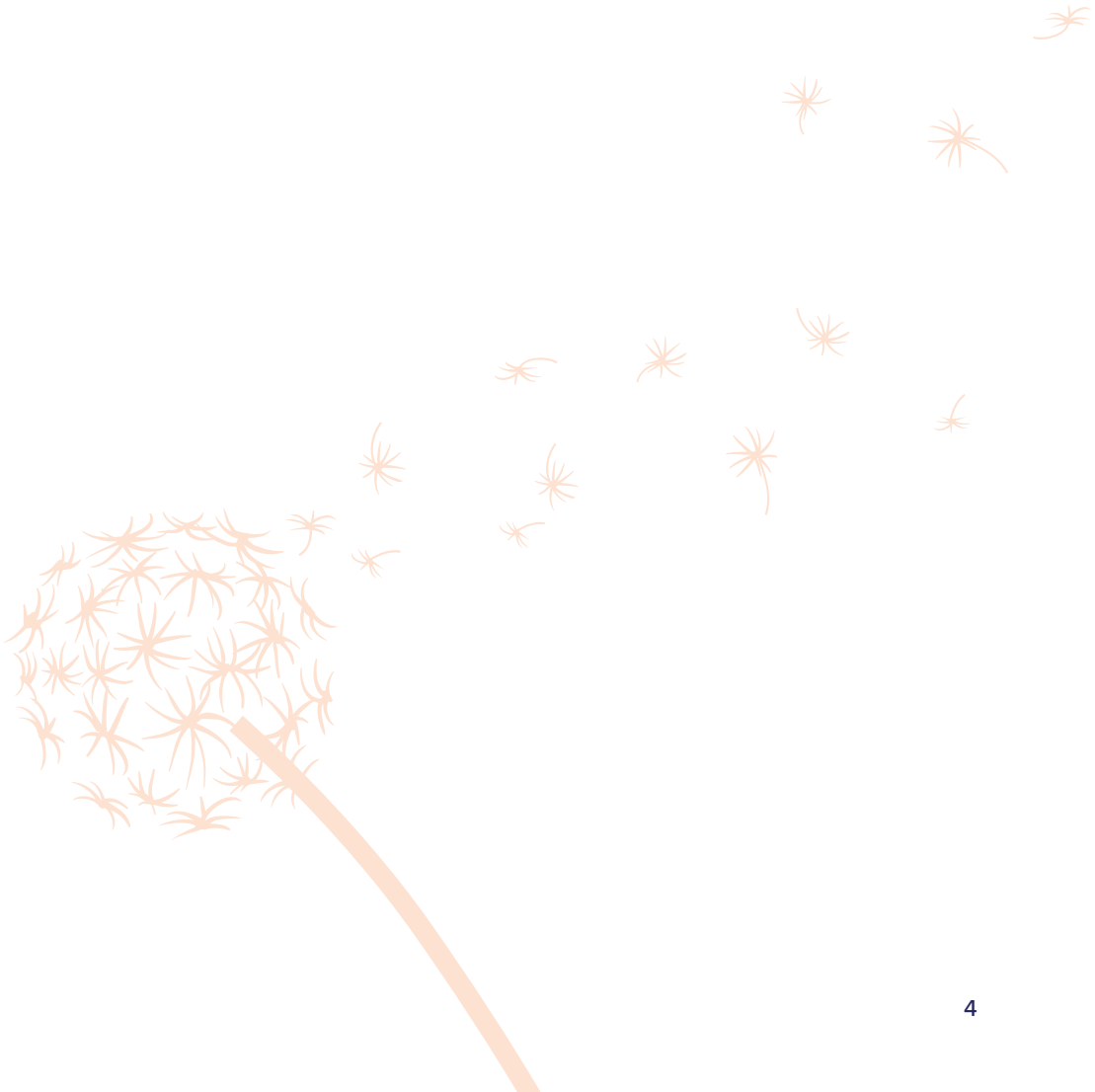
ANKARA
2023

COMPARATIVE STUDY ON DIGITAL RIGHTS
(GERMANY-AUSTRIA-IRELAND)

This document has been produced with the financial assistance of the European Union. The content of this document is the sole responsibility of the consortium led by WEglobal Danışmanlık A.Ş. and do not necessarily reflect the views of the European Union or the Ministry of Foreign Affairs Directorate for EU Affairs.

CONTENTS

LIST OF ABBREVIATIONS	
DPO	Data Protection Officer
DSA	Digital Services Act
EU	European Union
PET	Privacy Enhancing Technologies
TEU	Treaty on European Union



Prepared by
Assoc. Dr. Mehmet Bedii KAYA

1. Importance of Digital Rights

There have recently been important developments regarding digital rights in the European Union (EU or Union). To explain these developments, first an overview of the general framework in the EU will be provided, followed by a discussion of the concrete specific legal regulations.

At its inception, the Union adopted the principle of direct applicability for fundamental freedoms, enabling the free movement of goods and services. Legal harmonisation endeavours were primarily carried out through directives, which were generally binding only on member states, while regulations were the exception. Currently, the Union, as a prevailing trend, opts for regulations as a method of legal harmonisation, as they have direct applicability, especially in the digital field. Therefore, the Union proactively formulates its own normative parameters by minimising reliance on Member States for legislations. Moreover, the relevant regulations provide provisions named as 'opening clauses' endowing Member States with discretionary authority to diverge from the regulations in exceptional cases.

As a result of this trend, directives concerning digital rights available for transposition by Member States are frequently absent. Instead, the Union generally opts for regulations that can be directly applied in the national legal systems of Member States. In this regard, the legislative autonomy of Member States is notably limited. In addition, the Union provides for the simultaneous establishment of a relevant institution under each new regulation published regarding digital rights. This institution is mostly a new institution that does not yet exist in Member States. Therefore, discussions on Member States will primarily revolve around EU legislation and institutions that uniformly apply across all Member States. However, in exceptional cases where Member States are accorded discretion, information on state-specific legislation and institutions will be provided.

However, it is important to note that complete legal harmonisation does not necessarily imply harmonisation during implementation. Therefore, jurisdiction-specific discussions will focus on different practices, especially within the relevant Member State.

In the light of these general remarks, there are four primary legal instruments integral to the regulatory framework governing digital rights in the EU: the European Union Digital Single Market Strategy, 2030 Digital Compass Communication, Digital Decade Policy Programme Decision, and the European Declaration on Digital Rights and Principles for the Digital Decade.

The aim of the Digital Single Market Strategy is to contribute to economic growth, employment, competition, investment, and innovation within the Union based on three pillars. These pillars entail (i) ensure better access for consumers and business to online goods and services across Europe,, (ii) creating the right environment for digital networks and services to thrive, and (iii) maximising the growth potential of the European Digital Economy.

The 2030 Digital Compass Communication comprises four cardinal points: (i) fostering a digitally skilled population and highly skilled digital professionals, (ii) ensuring secure and performant sustainable digital infrastructures, (iii) facilitating the digital transformation of businesses, and (iv) promoting the digitalisation of public services.

The European Declaration on Digital Rights and Principles for the Digital Decade, particularly relevant to digital rights, is rooted in various principles. These principles are putting people at the centre of the digital transformation, promoting solidarity and inclusion, ensuring connectivity, facilitating digital education, training, and skills, establishing fair and just working conditions, providing digital public services online, safeguarding freedom of choice, addressing interactions with algorithms and artificial intelligence systems, fostering a fair digital environment, promoting participation in the digital public space, ensuring safety, security, and empowerment, creating a protected, safe, and secure digital environment, safeguarding privacy and individual control over data, protecting and empowering children and young people in the digital environment, and embracing sustainability. Noteworthy is that these principles partially overlap with other policy declarations mentioned earlier, while the European Declaration on Digital Rights and Principles drawing inspirations from fundamental rights and principles.

In this regard, the Union places people at the centre of digital transformation, aiming to ensure that technology serves and benefits all people residing in the EU by empowering them to pursue their aspirations, while fully safeguarding their fundamental rights and security. This people-centred approach is underpinned by the principles of solidarity and inclusion, stressing the unifying role of technology rather than its divisive nature. Moreover, the digital transformation should contribute to the establishment of a fair and inclusive society and economy in the EU. In terms of equality, the objective is to grant everyone in the EU access to affordable and high-speed digital connectivity. However, this necessitates the universal right to education, training, and lifelong learning, manifested in acquiring all basic and advanced digital skills. In the context of work life, everyone has the right to fair, just, healthy, and safe working conditions with appropriate protection in the digital environment as in the physical workplace, irrespective of their employment status, modality, or duration. With regards to digital public services, it is stated that everyone should have online access to key public services in the EU and data collection should be limited to what is strictly necessary for accessing such services. Concerning interactions with algorithms and artificial intelligence systems, one of the most important components of the digital world, artificial intelligence should function as a tool for individuals, aimed at improving human well-being. Therefore, everyone should be empowered to benefit from the advantages of algorithmic and artificial intelligence systems, making informed choices in the digital environment, while being protected against risks and harm to health, safety, and fundamental rights. Aligning with the principles outlined in the Declaration, everyone is entitled to choose effectively and freely which online services to use, based on objective, transparent, easily accessible, and reliable information. With regards to participation in the digital public space, the objective is to ensure that everyone has access to a trustworthy, diverse, and multilingual digital environment, promoting pluralistic public debate and effective participation in democracy without any discrimination. Particularly in matters of privacy and protection of personal data, another objective is to grant everyone access to digital technologies, products and services that are safe, secure, and privacy-protective by design, resulting in a high level of confidentiality, integrity, availability, and authenticity of processed information. It is set forth in the Declaration that everyone has the right to privacy and to the protection of their personal data, which includes the control by individuals on how their personal data are used and with whom they are shared. Another major issue pertains to the protection and empowerment of children and young people in the digital environment. In this regard, children and young people should be empowered to make safe and informed choices and express their creativity in the digital environment. In terms of sustainability, a pivotal topic in contemporary discourse, digital products and services should be designed, produced, used, repaired, recycled, and disposed of in a manner that mitigates negative impacts on the environment and society and avoids premature obsolescence.

In the constantly evolving legal landscape with both existing and newly introduced regulations, the next section will first explain the current legal framework, followed by the discussion of the upcoming regulations envisaged under the Union's Digital Policies.

In conformity with the legal framework established by the Treaty on European Union (TEU), its provisions must be considered as the primary legislation in force. Article 2 of the TEU emphasises that the Union is founded on a set of values comprising fundamental rights and freedoms, while the Article 6 recognises the status of fundamental rights and freedoms as general principles of EU law, stemming from the constitutional traditions common to Member States. The Charter of Fundamental Rights of the European Union, legally binding and equivalent to the Founding Treaties of the Union as stipulated in Article 6 of the Treaty on European Union, sets out the right to respect for private and family life under Article 7 and the right to the protection of personal data under Article 8 as fundamental rights and freedoms. Moreover, the Charter addresses non-discrimination under Article 21. Although these regulations stated in primary legal sources are very abstract, it is possible to see their reflections in the Union policies. Clearly, these fundamental rights are embedded in policies centred on human dignity, placing people at the centre, and adopting principles such as privacy, protection of personal data and the rule of law, especially regarding digital policies.

In terms of secondary legislation, this study will focus on each sector separately.

Initially, regarding infrastructural regulations, the general framework for connectivity is established through Frequency Bands Directive 87/372/EEC, (EU) 2015/2120 Open Internet Access Regulation, European Electronic Communications Directive (EU) 2018/1972, Roaming Regulation (EU) 2022/612, Union Secure Connectivity Programme Regulation (EU) 2023/588, and '.eu Top-Level Domain Name' Regulation (EU) 2019/517.

In the field of data protection and privacy, General Data Protection Regulation (GDPR) (EU) 2016/679 undoubtedly establishes a standard not only within the Union but also worldwide. Nonetheless, Union actions in this field are

beyond the scope of the GDPR. On the contrary, this Regulation is reinforced by the Regulation (EU) 2018/1725 which pertains to the protection of natural persons concerning the processing of personal data by the Union institutions, bodies, offices, and agencies. This regulation predicated on the personal data processing activities of the Union institutions and organisations. Moreover, Law Enforcement Directive (LED) (EU) 2016/680 introduces specific provisions for the personal data processing activities of law enforcement forces. This Directive is complementary to the GDPR. Regarding the protection of personal data in electronic communication, e-Privacy Directive 2002/58/EC incorporates specialised provisions addressing the use of cookies. It was intended to repeal this Directive with the Proposal for an e-Privacy Regulation, planned to coincide with the GDPR. However, 2002/58/EC, also known as the old Directive, remains in force due to the absence of agreement among Member States on the draft. Moreover, Free Flow of Non-Personal Data Regulation (EU) 2018/1807 and Open Data Directive (Public Sector Information - PSI) (EU) 2019/1024 are in force regarding the free circulation of data not qualifying as personal data. These enactments, contrary to the protection of personal data, aim to ensure the unrestricted flow of non-personal data. Another legislative instrument introduced to facilitate data flow and to obtain more added value from data in the digital economy is Data Governance Regulation (EU) 2022/868, also known as the European Data Governance Act (DGA). DGA aims to facilitate the use of datasets, especially those held by the public sector, by people concerned. The Data Act Proposal No. COM(2022) 68 final, which regulates the mandate to access data generated by individuals through connected devices, is pending adoption. In close connection with the Data Act and the DGA, the Proposal for a Regulation on European Health Data Space (COM(2022) 197 final) is additional legislative measure aiming to enable secure access to public health data under public control and supervision. Another legislative initiative targeting interoperability of Union institutions in the digital environment is the Proposal for a European Interoperability Regulation (Interoperable Europe Act) COM(2022) 720 final. Although this Regulation remains in the draft stage, it is predicated on the technical, administrative, and legal interoperability criteria of the Union institutions in the digital environment.

The first notable act regarding intellectual property is the Directive on the legal protection of databases 1996/9/EC (Databases Directive). Other important legal instruments in this field are Community Designs Regulation (EC) No 6/2002 and Directive (EU) 2016/943 on the Protection of Trade Secrets. Noteworthy among the anticipated regulations is the Proposal for a Compulsory Licensing Regulation COM(2023) 224 final.

In the field of cybersecurity, there are a few important acts include the EU Cybersecurity Act (EU)2019/881, Regulation (EU)2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre, and Network and Information Security Directive (EU) 2022/2555 (NIS 2 Directive). The proposed acts in this field are the Proposal for an Information Security Regulation COM (2022) 119, the Proposal for a Cybersecurity Regulation COM (2022) 122, the Proposal for a Cyber Resilience Act COM (2022) 454, and the Proposal for a Cyber Solidarity Act COM(2023) 209 final.

Regarding product safety, General Product Safety Regulation (EU) 2023/988 is important. In addition, especially regarding artificial intelligence, noteworthy drafts include the Proposal for an Artificial Intelligence Act COM/2021/206 final and the Proposal for an AI Liability Directive COM (2022) 496.

E-Commerce/Consumer Protection has always been one of the issues highly prioritised by EU legislators. Although the absence of specific provisions tailored for the digital markets within preceding enactments in this regard, there has been a notable increase in the number of legislative acts explicitly addressing matters pertaining to digital markets. Noteworthy examples include Geo-Blocking Regulation (EU) 2018/302, Digital Content Directive (EU) 2019/770 and especially Digital Services Act (EU) 2022/206.

In the field of competition law, P2B Regulation (EU) 2019/1150 and Digital Markets Act (EU) 2022/1925 stand out. Both legislative acts encompass vital provisions specifically aimed at regulating competition in the digital space.

In the field of finance, Payment Services Directive 2 (PSD2) (EU) 2015/2366 and Crypto Assets Regulation (MiCA) (EU) 2023/1114 stand out prominently as noteworthy enactments within the realm of digital rights. Moreover, Digital Operational Resilience Regulation (DORA) (EU)2022/2554 distinctly focuses on digital markets. Lastly, the Proposal for a Digital Euro Regulation COM (2023) 369, the Proposal for a Financial Data Access Regulation COM (2023) 360 and the Proposal for a Payment Services Regulation COM (2023) 367 should also be noted.

2. Selected Member States

All these developments regarding digital economy within the Union encompass, numerous enactments directly or indirectly related to digital rights. Three Member States-Germany, Austria, and Ireland- are specifically chosen for examination regarding the impact of these enactments at the national level.

Due to its economic power of Germany, its population and its important role in shaping Union law, Germany stands as a primary exemplar. Well before the adoption of Union-level enactments, especially in areas such as data protection law, Germany started to regulate these issues in both legislation and case law. This makes German legislative and jurisprudential practices a notable example worthy of discussion.

Austria, despite being a medium-sized or even small-sized country, is a crucial as an illustrative example. The primary factor for selecting Austria is its legal practices with numerous cases related to digital rights and, particularly, the protection of personal data brought before the Court of Justice of the European Union at the request of the Austrian Supreme Court for a preliminary ruling. The underlying reason is that the active engagement of digital rights activist Max Schrems and his organization 'NOYB' operates from Austria. Therefore, Austria stands out as a pertinent choice.

Finally, the selection of Ireland is grounded in its favourable tax policy since the early 2000s, drawing the attraction of global technology companies to establish their European bases in the country. Ireland frequently serves as the epicentre for investigations against many technology giants such as 'Alphabet', 'Meta' and 'TikTok'. For this reason, Ireland was particularly deemed worthy of discussion.

3. Legislation Enacted by Member States for Harmonisation

As stated above, notwithstanding the historical preference to use directives in the digital field, the presently favoured legal instrument is regulation. The European Commission states the reason behind this trend as the inadequacy of achieving harmonisation through directives. The most striking example of this paradigm shift is the preference for a regulation to revise Directive 95/46/EC regarding personal data protection, in the alignment with contemporary needs. Moreover, a regulation is expected to replace Directive 2002/58/EC on e-privacy. Data Governance Act, Data Act Proposal, Artificial Intelligence Act Proposal are all prepared in the form of regulations.

As is known, regulations, unlike directives, do not address Member States and require them to transpose the legislation of which the general framework is drawn up. On the contrary, in case of regulations, being the most effective form of harmonisation, albeit affording the least discretion to Member States, the provisions are directly implemented across all Member States. Therefore, in cases where EU law is applied, the level of discretion given to Member States in terms of digital rights is quite narrow. Since regulations are directly implemented, the issues in the same field on which Member States can provide for provisions are very limited.

This study examines the Union enactments pertinent to certain fields that directly impacting digital rights, with a primary focus on their implementation within Member States. The selected fields are personal data protection law, data governance law, digital markets law, electronic commerce law and cybersecurity law. It is worth emphasising that that it is not possible to separate these fields from each other in any definitive way. On the contrary, since these fields are interconnected, there will be many instances of overlapping.

3.1. Personal Data Protection Law

The first legislative instrument within the Union framework dedicated to protection of personal data is the now-repealed Directive 95/46/EC. This Directive was promulgated when the Internet was not yet available in every home and when mobile phones, tablets and even personal computers were not yet widespread, before the emergence of social media. However, in the late 90s and early 2000s, as personal computers become more widespread and the Internet became a common aspect of everyday life, lawmakers began considering the revision of rules regarding cross-border data transfer. As the close cooperation of companies operating within the Union and American counterparts extends into the digital field, the relevance of Directive 95/46/EC began to increase. One of the most prominent examples of this nexus is the merger of the German automotive manufacturer Daimler AG with the American Chrysler. This corporate fusion necessitated the transfer of substantial volume of personal data to the United States. In order to solve this problem, 'Binding Corporate Rules', clearly regulated under the GDPR were adopted as a result of the cooperation between data controllers and Member State authorities. Then, with the emergence of social media, challenges not only arose in cross-border transfer of personal data but also in the analysis of data for many different purposes, especially for commercial endeavours. Although cloud computing holds appeal for numerous commercial companies, it also causes many problems in terms of data protection law. In response to these developments, the Article 29 Data Protection Working Party[1], comprising representatives from the data protection authorities of all Member States, issued guidelines, thereby elucidating the implementation of pertinent regulations. Consequently, the need to revise the Directive arose. After long discussions, the GDPR entered into force in May 2016, with its operative implementation was scheduled for the conclusion of the designated 2-year transition period granted to Member States, which concluded in 2018.

First, the GDPR diverges from a formal procedural approach concerning personal data, opting instead for a risk-based methodology. This legal framework introduces a novel legislative paradigm applicable to both legal subjects and regulatory authorities. More clearly, regulatory authorities, especially in the digital field, exhibit an inherent information asymmetry compared to private enterprises. This informational discrepancy contradicts the mandatory legislative rationale; effective regulation and monitoring depend on the regulatory authority's comprehensive understanding of the subject matter. However, in the digital field, it is often possible to determine that many addressees only formally fulfil the requirements of the law and do not really establish a life cycle beyond that. The information asymmetry between public authorities and private enterprises as well as the addressees being satisfied with a formal approach, led to a change in the law-making logic. According to this logic, the addressees of the law will first determine the risk arising from their own activities. Thus, the risk of information asymmetry will be minimised. So, what happens if the data controller or data processor miscalculates or fails to calculate this risk? At this stage, another very important new principle introduced by the Regulation stands out: accountability. This means that although the data controller or processor may be able to determine their own risk, they are held accountable if the relevant authority investigates in case of violation of data protection law. In other words, they must be able to explain which measures they take and why and be accountable. Thus, contrary to the classical imperative regulatory logic, each data controller (and data processor) may now determine their own risk, may take the necessary measures to mitigate the risk, and may document their actions when necessary. This foundational approach can be seen in various places under the EU General Data Protection Regulation.

First, accountability emerges as a fundamental principle articulated within the general principles provisions of the GDPR. Therefore, this principle must be respected in all kinds of data processing activities. Moreover, accountability should not be deemed solely as being accountable to authorities. On the contrary, it extends to the relevant individuals whose personal data is subject to processing. In this respect, it is also of great importance in terms of data subject rights and therefore digital rights to ensure that the privacy policies and explicit consent texts should be understandable, and the principles of privacy by design and privacy by default should be taken into account, and privacy enhancing technologies (PET) should be used. The GDPR grants the data subject the right to withdraw their explicit consent at any time, the right to object in cases of personal data processing based on legitimate interest, and the right to request a copy of the personal data subject to processing. The latter particularly underscored in recent decisions by the Court of Justice of the European Union.

The impacts of adopting a risk-based approach under the GDPR is evident prominently in administrative and

1 With the entry into force of the EU General Data Protection Regulation, this working party was succeeded by the European Data Protection Board (EDPB).

technical measures. More specifically, in accordance with this principle, data controllers in some cases and the public authorities in all cases are obliged to designate a Data Protection Officer (DPO), and they are required to carry out a Data Protection Impact Assessment, especially where data processing activities are likely to result in a high risk.

To increase legal security and promote standardisation and harmonisation, the Regulation also encourages the development of data protection standards and sector-specific Codes of Conduct. Thus, the provisions of the Regulation, which contain many abstract concepts, are materialised thanks to these standards, sector-specific interests are taken into account and finally legal security is established.

As stipulated, enactments regarding the protection of personal data are not exclusively limited to the GDPR. There are special regulations across various fields. The most important among these is Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, commonly referred to as ePrivacy Directive. The Directive has caused many debates in practice, especially due to the provisions regarding data packages called cookies and their placement on terminal equipment. The Directive intended to be revised concurrently with the GDPR, however, the envisaged update has not materialised, as Member States have yet to reach a consensus on the ePrivacy Regulation Proposal.

3.1.1. Germany

Under German legal framework, each federal state has its own legislation concerning the protection of personal data. Moreover, the Federal Data Protection Act (Bundesdatenschutzgesetz) remains in force at the federal level although its scope of application has been severely limited after the enactment of the GDPR. In this context, especially provisions regarding data processing for employment-related purposes (§ 26), data processing for scientific or historical research and for statistical purposes (§ 27), data processing for archiving purposes in the public interest (§ 28), consumer loans (§ 30) and scoring and credit reports (§ 31) are still applicable.

Regarding the transposition of the ePrivacy Directive, the Law on data protection and the protection of privacy in telecommunications and telemedia (Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien, TTDSG) came into force on 1 December 2021. With this enactment, aligning with the Planet49 decision, the legal mandate for obtaining explicit consent for cookie processing via the opt-in method has been established.

3.1.2. Austria

In Austrian law, the Federal Act concerning the Protection of Personal Data (Datenschutzgesetz – DSG) is in force, subsequent to the enactment of the GDPR. This law primarily regulates the data processing activities of public authorities and stipulates provisions for specific cases (processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes).

3.1.3. Ireland

The Irish Data Protection Act (2018) remains in force alongside the GDPR, like the German and Austrian law. The Act includes provisions regarding the data processing activities of public institutions and organisations as well as regarding the organizational structure of the Data Protection Authority. The Act also introduces specific provisions regarding the protection of children's personal data. There are also provisions regarding the protection of special categories of personal data during the investigation and prosecution.

3.2. Data Governance Act

The approach in formulating provisions regarding data has traditionally focused on the protection of personal data. However, since the most important raw material of the digital economy is data, the Union has gone one step beyond limiting data only to personal data and making arrangements to exclusively protect such data, and has provided for important provisions, especially to encourage the usage of non-personal data.

The first of these regulations is the Data Governance Act (EU) 2022/868. The Data Act (COM (2022) 68), which is still a draft text, is also of great importance. Both acts are to secure the circulation of existing data, facilitating data access for small and medium-sized businesses and entrepreneurs, especially those operating in the field of digital economy. Additionally, they aim to provide individuals, as the direct producers of the data, ownership rights over their respective data.

The Data Governance Act essentially pursues three main objectives: (1) Facilitating access to data held by public bodies for individuals, (2) Establishing the general framework for joint data utilisation, and (3) Ensuring the use of data for the public benefit (data altruism).

It should be pointed out that access to data on which no one claims rights is currently regulated within the framework of the Open Data Directive. The Data Governance Act aims to establish a comprehensive framework for ensuring access to data that public bodies are hesitant to provide to third parties due to intellectual property rights, trade secrets or protection of personal data. However, the Act does not impose any obligation on public authorities to provide data access. Authorities may establish the necessary technical and administrative infrastructure to share the data they hold with relevant persons, using all necessary techniques, provided that they do not violate legal protection.

Moreover, there are already 'data pools' created by multiple enterprises in practice. These seem to be a mechanism enabling actors operating in the same sector to share information among themselves. The purpose of the Act is to encourage the formation of these information pools, create safe environments and facilitating access to data. As a concrete example, the Proposal for a European Health Data Space Regulation (COM(2022) 197 final) was issued. This Proposal aims to collect health data in a secure environment under public supervision and present such data to relevant persons after necessary inspections.

The Proposal also aims to establish and develop data altruism to ensure the circulation of data, establishing a registry mechanism in this context, and to create explicit consent texts.

Finally, the Act provides for the establishment of the European Data Innovation Board to ensure control, supervision and especially coordination.

While the Data Governance Act establishes the institutional framework of data governance, the Data Act regulates individuals' access to data they produce. After a long negotiation process, agreement was reached on the Data Act. It is expected to become law by the end of 2023.

The main purpose of the Data Act is to ensure access to the data obtained from devices through connected products or services by the individuals who 'produce' them. In this regard, the connected product or service will either provide access to the data produced directly or where this is not possible, the individual will always be able to request access to the data obtained as a result of their own use. Moreover, the direct transfer of this data to third parties can also be requested in the same manner. For this purpose, the Act provides for a contract between the producer and the individual regarding the data to be obtained and made available. Therefore, when any connected product or device that produces data is purchased, a 'data license agreement' must be signed between the buyer and the producer. If such data is transferred from one producer to another, a new license agreement must be signed.

An important conclusion from the aforementioned is that the EU directly resorts to private law principles to attain many numerous objectives acknowledged within the legal policy context. It intervenes the freedom of contract, compelling parties to conclude a contract, and also determines the minimum content of such contract. The Data Act contains provisions under the title of unfair terms regarding the data license agreement to be concluded between the manufacturer and another manufacturer to whom the data will be transferred upon the request of the customer. On the other hand, there is no distinct provision regarding the contract to be concluded between customers and the manufacturer. The reason behind this is that the Unfair Contract Terms Directive, which comprehensively regulates the general transaction conditions, already contains sufficient provisions.

In order to strengthen competition between actors in the data economy, provisions have also been introduced to allow customers to transfer data between data processing service providers. Accordingly, any hinderance related to transmission of data from one service provider to another is deemed invalid.

Finally, the Regulation introduces important obligations in terms of interoperability regarding facilitating the transition between different systems.

3.3. E-Commerce and Digital Services

The main enactment regarding electronic commerce is Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). The following statements are made in the Recitals regarding the impact of the Directive on fundamental rights and freedoms: (Recital (9)): *The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.*

The purpose of the Directive is to contribute to the proper functioning of the internal market by ensuring the free movement of information society services among Member States. To achieve this, the Directive seeks to harmonise certain national provisions on information society services related to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, extrajudicial dispute resolution, legal actions, and cooperation between Member States.

In accordance with a fundamental principle of the Directive, also known as the country of origin principle, Member States are prohibited from restricting the freedom to provide information society services from another Member States within coordinated field. Additionally, Member States are required to guarantee that the engaging in the activities of an information society service provider is not subject to prior authorisation or any other equivalent requirement.

According to another obligation in this regard, Member States must ensure that their legal system permits the conclusion of contracts through electronic means. Member States are in particular required to ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of them having been made by electronic nature.

Another important rule adopted is regarding the nonliability of intermediary service providers.

The act regarding digital services within the Union, and hence directly effecting digital rights is the Digital Services Act (EU) 2022/2065 (DSA). The Act introduces important obligations for digital service providers. However, these obligations are not equal for every service provider. More specifically, much stricter rules are provided for enterprises categorised as large online platforms, also known as GAFA (Google, Apple, Facebook and Amazon), while smaller enterprises are subject to simpler obligations. These obligations encompass the removal of illegal content, appointment of a legal representative, incorporation of service restrictions in the terms of use, transparent implementation of these restrictions in an objective, proportionate and responsible manner; disclosure of content control activities; notification to judicial and law enforcement authorities, adherence to 'know your business customer' (KYBC), advertising transparency, conducting risk assessments; undergoing independent auditing and appointing a compliance officer; ensuring transparency of recommender systems. Moreover, the Act provides for significant fines in case of violation of these obligations. To this end, in case of violation of the DSA, interim measures, or commitment decisions, fines of up to 6% of the annual turnover may be imposed. Moreover, for the provision of incorrect, incomplete, or misleading information, fines of up to 1% of the annual worldwide turnover may be imposed. Finally, daily fines, until compliance) may not exceed 5% of the average daily turnover of the intermediary service provider.

3.3.1. Germany

German law does not contain any uniform law regulating electronic commerce. Instead, the provisions of § 312 b ff in the German Civil Code (Bürgerliches Gesetzbuch) regulate this issue. Moreover, the Telemedia Act (Telemediengesetz, TMG) also contains important provisions. In addition, the Signature Act (Signaturgesetz, SigG), the Price Indication Regulation (Preisangabenverordnung, PAngV) and the Consumer Dispute Resolution Act (Verbraucherstreitbeilegungsgesetz, VSBG) are among the important acts in this field.

3.3.2. Austria

Austria regulates the online sale of goods and services by two fundamental laws.

The Distance and Off-Premises Contracts Act (FAGG) emerged as a result of the implementation of the Consumer Rights Directive, and covers every contract between an enterprise and a consumer concluded outside the enterprise's premises, but through a distance sales or service distribution system (e.g. websites), or generally concluded remotely. FAGG sets out both pre-contractual and post-contractual information obligations, including the description of the basic features of the goods/service, delivery and service conditions, and the consumer's right of withdrawal.

Austria additionally enacted the E-Commerce Act (ECG) as a result of the implementation of the E-Commerce Directive. The ECG includes general information obligations (e.g. name, address, at least two contact options, competent regulatory authority), information obligations in advertising (e.g. clear recognition of the ad, recognition of the advertiser) and information obligations on websites (e.g. information of the technical steps of the ordering process).

Moreover, other information and disclosure obligations are provided for in the Companies Act (UGB), the Professional Act (GewO) and the Media Act (MedienG).

3.3.3. Ireland

In Ireland, the legislation is directly implementing Directive 2000/31/EC is the S.I. No. 68/2003 - European Communities (Directive 2000/31/EC) Regulations of 2003. This regulation imposes specific obligations on online businesses, including the requirement to present their products and services clearly and correctly, enable consumers to cancel orders easily, and take measures to protect consumers from fraud. The Regulation also sets out for measures for businesses to protect the privacy of customers' personal data. Accordingly, enterprises are required to obtain permission from customers before collecting or processing their personal data and to securely store such data. In this regard, the following obligations are particularly important:

Information obligations: Enterprises are obligated to present their products and services transparently and accurately, providing their identity, contact information and geographic address. They must also state the terms and conditions of their contracts and the methods they use to process payments.

Cancellation Rights: Consumers have the right to cancel orders for goods or services without providing any reason within seven days after receiving them. Moreover, businesses must inform consumers of their cancellation rights and make it easy for them to exercise these rights.

Prevention of Fraud: Measures to prevent fraud, such as ensuring the security of their websites and prohibiting the acceptance of payments from unauthorised third parties.

Data Protection: Businesses are obligated to take measures to protect the privacy of their customers' personal data. This means that enterprises are required to obtain permission from customers before collecting or using their personal data and ensuring secure storage of such data.

3.4. Cybersecurity Law

The most important act at the Union level regarding cybersecurity, which is important for the protection of digital rights, is the Network and Information Security Directive (NIS 1). The Directive lays down measures seeking to achieve a high common level of security of network and information systems within the Union to improve the functioning of the internal market. The Directive respects the fundamental rights recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This principle is also required to be observed in the implementation of the Directive.

In line with this general purpose, operators of essential services are defined. These operators consist of operators active in the following sectors: energy, electricity, oil, gas, transport, road transport, rail transport, air transport and water transport, banking, financial market infrastructures, health, drinking water supply and distribution, digital infrastructure, IXPs, DNS service providers and TLD name registries. Digital service providers are also defined. These providers consist of businesses active in online marketplace, online search engine and cloud computing service.

These actors are required to ensure cybersecurity. To this end, they must take risk-appropriate and operational measures to prevent the risk or mitigate its effects. These actors are also mandated to ensure the security of network and information systems and reporting cybersecurity incidents.

The Network and Information Security Directive (NIS2) defines operators of essential services and important operators, followed by highly critical sectors. These sectors are as follows: energy (electricity, district heating and cooling, oil, gas, hydrogen), transport (air, rail, water, road), banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management (business-to-business), public administration and space. Other critical sectors are listed as postal and courier services; waste management; manufacture, production, and distribution of chemicals; production, processing, and distribution of food; manufacturing; digital providers and research. Moreover, the Directive encompasses various sectors; digital services such as electronic communication service providers, social network providers and data centre services; wastewater and waste management; manufacturing of some critical products (pharmaceuticals, medical devices and chemicals); postal and transportation services, food, and public administration services.

The basic obligations introduced under the Directive can be summarised as cybersecurity incident management and crisis management, vulnerability management and disclosure, evaluation of the effectiveness of risk management measures, basic cyber hygiene practices and cybersecurity training, effective implementation of cryptography, human resources security, access control policies, and asset management.

Regarding fines, the Directive stipulates administrative fines, with a maximum of at least EUR 10,000,000 or at least 2 % of the total worldwide annual turnover, whichever is higher.

3.5. Artificial Intelligence Law

In April 2021, the European Commission published the Proposal for an Artificial Intelligence Act COM/2021/206 final, which proposes a horizontal framework for artificial intelligence systems. The AI Act aims to classify the artificial intelligence systems within the Union based on their risk levels, protecting fundamental rights and freedoms, and upholding the public interest. The Act also emphasised that artificial intelligence systems must be align with ethical, transparent, accountable, and human-centric principles.

In order to achieve these objectives, various rules are proposed in the Proposal, including addressing the potential risks that artificial intelligence systems may cause in the context of fundamental rights and freedoms; classification of high-risk AI systems; identifying clear requirements for high-risk AI systems; defining special obligations for providers of high-risk AI systems; ensuring that high-risk AI systems undergo a conformity assessment procedure, prior to their placing on the market or putting into service; conducting risk assessments of AI systems which continue after being placed on the market; and establishment of a governance structure at Union and national level.

As the first comprehensive and general initiative to regulate artificial intelligence worldwide, the AI Act sets a critical precedent for future AI regulatory frameworks. Several aspects of the Proposal will provide insights for other legislative bodies. These are the application of a risk-based approach; the comprehensive definition of artificial intelligence; the scope of rights granted to individuals and enterprises; allocation of responsibility considering the complexity of artificial intelligence systems and decision-making processes; how future-proof approach of the act; the scope of risk categories; prohibited use of AI cases; and how to find a balance between the interests of big tech and the public interest.

In light of these general explanations, the Proposal defines 4 risk levels for AI systems:

a. Unacceptable Risk

From social scoring by governments to voice assistance built-in toys that encourage dangerous behaviour, any AI system deemed a clear threat to public security and to livelihoods and rights of persons will be prohibited.

b. High Risk

High-risk AI systems cover various areas such as critical infrastructures, education, product safety, employment, public services, law enforcement, migration, justice, and democratic processes. These systems must meet strict obligations before being placed on the market.

c. Limited Risk

Limited risk refers to AI systems with specific transparency obligations. When utilising AI systems such as chatbots, users must be aware that they are interacting with a machine so they can make an informed decision to continue or step back.

d. Minimal or No Risk

The framework allows the free use of minimal-risk AI. This includes applications such as AI-powered video games or spam filters. The vast majority of AI systems currently used in the EU fall into this category.

The most important category among the four delineated risk categories, undoubtedly, pertains to high-risk AI systems. In this regard, the Proposal sets out substantial obligations. These obligations can be divided into three main categories: conformity assessments, technical infrastructure and inspection, and post-marketing monitoring requirements.

A significant portion of the prescribed obligations pertains to the natural or legal person who places the AI system on the market or makes significant modifications to the product already placed on the market. However, considering the Proposal's approach encapsulating the entire life cycle of AI systems, it also provides for obligations for users, importers, distributors and notified bodies.

Regarding the monitoring of compliance with these obligations, Member States will be responsible for overseeing the practices and sanctions of the supervisory authorities. A 'European Artificial Intelligence Board' composed of representatives from Member States and the Commission will be established to offer recommendations to national supervisory authorities. The Board will provide advice and assistance 'with regard to matters covered by this Regulation'. In addition, the Board may invite external experts and observers to attend its meetings and may hold exchanges with interested third parties.

As for penalties, a mechanism based on risk category is envisaged. In this regard, the heaviest fines, reaching up to 35 million Euros or 7% of turnover, are to be applied for the use of prohibited AI systems. For high-risk AI systems, the upper cap for violation of obligations is set at 15 million Euros or 3% of the turnover. Failure to provide accurate and complete information to national authorities may result in fines up to 7.5 million Euros or 1.5% of turnover. It should be noted that the regulation is still in the draft stage and these fines are subject to potential change. An agreement has been reached on the Act between the Council and the Parliament, and it is expected that the proposal will be enacted into law in 2024:

4. Institutional Structures at Union and National Level

As stated above, many legislative acts introduced in the field of digital economy are now prepared as regulations. The establishment of new European Union structures is envisaged. First, the institutions that are planned to be established in the above-mentioned fields will be discussed in detail. However, instead of directly imposing fines, these institutions mostly perform regulatory activities and undertake the task of ensuring coordination between different authorities of Member States. Therefore, institutional structures within Member States still holds great importance regarding the implementation of EU law in Member States. To this, institutional structures active in the fields of data law, electronic commerce and digital services, and cybersecurity will be examined focusing on selected Members.

4.1. Existing and Planned EU Institutions

The EU acts explained in detail above provide for the establishment of new institutions in many areas. In accordance with these acts, the institutions are as follows:

Establishing a European Artificial Intelligence Board under the Proposal for an AI Act. Regarding data governance, European Data Innovation Board is anticipated to be established under the Data Governance Act. According to the GDPR, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have already been established. Finally, regarding cybersecurity, the authorised bodies, namely the European Cybersecurity Industrial, Technology and Research Competence Centre and the European Union Agency for Cybersecurity (ENISA), are important.

4.2. Germany

Due to Germany's federated structure, each federal state has its own data protection authority in data protection law. These state authorities are responsible for the supervision and control of data protection activities within their respective states. There is also the Federal Data Protection Authority operates at the federal level. However, in Germany, state authorities play a pivotal role in regulatory procedures, inspections and especially fines.

These state authorities are directly authorised to implement the GDPR. However, in exceptional cases where the EGDPR grants Member States the authority to establish provisions under the 'opening clause', the respective state data protection authorities serve as the competent authorities.

There is also an organization called Data Protection Conference (Datenschutzkonferenz (DSK)) authorised to facilitate cooperation between authorities. This organization, just like EDBP, provides recommendations, makes decisions, ensures coordination between different authorities, and publishes guidelines on implementation.

In terms of data governance, there is currently no established authority at the national level. Therefore, a central institution should be primarily established to regulate data governance concerning information held by the public authorities. Moreover, a separate institution should be designated for the control and supervision of data intermediary services. However, this authority should differ from the authorities responsible for data protection, competition, and cybersecurity (Article 13 f. 3 DGA). Finally, it will be essential to establish a registry and identification a competent authority in terms of data altruism.

Various institutions hold authority in the field of electronic commerce and digital services. The first of these is the Federal Network Agency (Bundesnetzagentur), authorised under the telecommunications and telemedia laws. In addition, there are the following authorised bodies include Financial Supervisory Authority (Finanzdienstleistungsaufsicht, BaFin) regarding payment services, Federal Cartel Office (Bundeskartellamt) on unfair competition, Federal Office of Consumer Protection and Food Safety (Bundesamt für Verbraucherschutz und Lebensmittelsicherheit) focusing on consumer rights, and finally Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) responsible for cybersecurity.

The Federal Office for Information Security is a federal agency under Germany's Ministry of Interior. BSI is responsible for the security of information technology systems and networks in Germany. It offers consultancy, support and training to private enterprises, public authorities, and individuals. It is also in charge of developing safety standards and guidelines. To this end, BSI is authorised to provide consultancy and support to companies, administrations, and individuals on information security; to develop safety standards and guidelines; to conduct information security audits; to warn against information security risks; and to raise public awareness about information security.

4.3. Austria

The competent authority for data protection law in Austria was previously the Data Protection Commission (Datenschutzkommission). However, due to its organizationally affiliation with the Ministry of Justice, the Court of Justice ruled in its decision of 16 October 2012, that this authority lacked independence, thereby failing to comply with Directive 95/46/EC. Following this decision, Austria established a completely independent authority, the Data Protection Authority (Datenschutzbehörde). The Data Protection Authority of Austria operates in accordance with the data protection regulations and the data protection legislation for criminal investigations. The Data Protection Authority is completely independent in performing its duties and exercising its powers. Among the various tasks of the Data Protection Authority are, in particular, to consider data protection complaints and conduct official investigations and administrative enforcement investigations; and cooperate with other data protection authorities in cross-border situations within the EU or the European Economic Area (EEA). The Federal Administrative Court serves as the appellate and complaint authority against the decisions of the Data Protection Authority. The Federal Administrative Court evaluates the decisions of the Data Protection Authority, as well as complaints and appeals where the Data Protection Authority fails to fulfil its obligation to make decisions.

The explanations provided for the German legal framework regarding data governance law are equally applicable to Austria.

In the field of e-commerce, § 30 of the E-commerce law (Bundesgesetz, mit dem bestimmte rechtliche Aspekte des electronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz – ECG) grants the authority to the Ministry of Traffic, Innovation and Technology regarding electronic commercial messages, the Ministry of Justice regarding transparency and cooperation with other institutions, and the Ministry of Justice and the Ministry of Economy and Employment regarding all other obligations.

Finally, four other institutions have authority regarding cybersecurity. These are the Prime Ministry, the Ministry of Internal Affairs, the Ministry of Defence, and the Ministry of Europe and Foreign Relations.

4.4. Ireland

The authority responsible for data protection in Ireland is the Data Protection Commission. The Commission's jurisdiction covers the GDPR and the LED, as well as the Irish ePrivacy Regulation of 2011, which is Ireland's regulation regarding e-privacy. The duties, powers and matters related to the establishment of the authority are laid down in Articles 9 to 27 of the Data Protection Law of 2018.

The authority for the regulation of electronic commerce is vested in the Ministry for Enterprise, Trade and Employment.

In terms of cybersecurity, the Irish National Cyber Security Centre must be mentioned. Established in 2011, the National Cyber Security Centre (NCSC) is the government agency responsible for network and information security. The NCSC plays a pivotal role in managing major cybersecurity incidents, offering guidance and advice to citizens and businesses, and overseeing cybersecurity risks to key services. Aligning with counterparts in other EU Member States, the NCSC has adopted a proactive approach in various areas. The Computer Security Incident Response Team (CSIRT) under the NCSC manages risk and incident management in the public authorities. The responsibilities of the CSIRT include monitoring incidents at a national level; providing early warning, alerts, announcements, and dissemination of information to relevant stakeholders about risks and incidents; responding to incidents; and delivering dynamic risk and incident analysis and situational awareness.

5. Examples of Implementation

Although the EU prefers the Regulation as the legislative instrument to ensure the unification of acts; authorities of Member States and their practices play a crucial role in the implementation of these acts. To this end, this section will delve into the developments in Member States regarding digital rights, a subject that is particularly debated within the Union.

5.1. Germany

Regarding digital rights, various decisions made in Germany and extending to the Court of Justice of the European Union are important.

The first two of these decisions are Facebook-Fanpage (C-210/16 - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH) and Fashion-ID (C-40/17 - Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV). In the Facebook-Fanpage decision, an educational enterprise engages in various educational activities on Facebook, and in the Fashion-ID decision, a commercial enterprise transfers some of its visitor data directly to Facebook through the use of the Facebook-Like Button on its website. In return, Facebook shares statistical data with these enterprises about people who visit their sites, but does not share the identity of the visitors or any data that makes them identifiable. In both cases, the relevant data protection authorities took action on the basis that the relevant site operators together with Facebook were liable. The trial process initiated by the parties who appealed the decision, leading to adjudication by the Court of Justice of the European Union. The Court determined that although website operators do not have direct access to visitor information, they are joint data controllers with Facebook due to their shared pursuit of commercial purposes.

Another development concerning online environments is the decision Planet-49 (C673/17 - Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH). In this decision, it was debated that although the German law transposed Directive 2002/58/EC, it was not clear whether explicit consent for cookies should be obtained by opt-in or opt-out method. In its decision, the Court ruled that consent, as required to be obtained in the context of the EU General Data Protection Regulation and the ePrivacy Directive, cannot be implied. On the contrary, an active behaviour of the relevant individual is necessary. As a result of this decision, within the Union, a distinction was made between mandatory, statistical and marketing cookies on many websites, and websites started offering users the option to give explicit consent or reject these cookies, especially regarding statistical and marketing cookies.

Another important development pertaining to the penalties imposed under the General Data Protection Regulation. In one of its decisions, the Berlin Data Protection Authority imposed a fine of 15 million Euros against a company named Deutsche Wohnen SE. The company appealed to the Berlin State Court, which ruled that, under the German Misdemeanour Act, penalties against a legal entity require the determination of fault on the part of the relevant legal entity's organ or a natural person authorised to represent. As a result, the Court annulled the fine entirely. Subsequently, during the appeal phase of the decision, the Berlin State Supreme Court referred the case to the Court of Justice of the European Union as a preliminary question (C-807/21). The Court has not yet awarded a final decision. However, the prosecutor's stance on the case asserts that legal entities may be directly subject to the penalties outlined in the General Data Protection Regulation. Additionally, legal entities may be held liable for the acts of persons who are not members of the management body or who do not have the authority to represent. It has also been argued that an objective violation is sufficient for this. This discussion on the legal nature of the penalties stipulated in the EU General Data Protection Regulation and other acts hold great significance, both regarding data protection law as well as regarding all acts in the digital field that provide for heavy penalties.

Another pertinent issue for Germany is the dispute between Meta and the Federal Cartel Office (Bundeskartellamt). Following Meta's announcement that it would combine the data collected from Facebook, WhatsApp and Instagram; the German Cartel Office prohibited this activity, and Meta subsequently took legal action.

Therefore, the data protection law is not limited exclusively to the jurisdiction of data protection authorities, and it has been decided that competition authorities may be authorised in cases involving behaviour that disrupts competition and constitutes unfair competition.

5.2. Austria

There have been significant developments in data protection law and e-commerce in Austria. The first of these developments concerns the decision C-300/21 – Österreichische Post/UI of the Court of Justice of the European Union. The legal issue examined in the relevant decision is whether the violation of the General Data Protection Regulation is sufficient to award compensation. In its decision, the Court ruled that mere violation of the General Data Protection Regulation is insufficient to claim material or moral compensation, that the illegal act must cause damage and a causal link must be established between the tort and the damage. Moreover, the Court stated that any negative emotion/thought/feeling does not constitute harm, emphasising that the competent courts of Member States should consider the principles of equivalence and functionality when calculating compensation. This decision is particularly important in terms of digital rights. In fact, to effectively protect the rights and freedoms of individuals, the data protection law confers the authority to administrative authorities to impose penalties while giving the right to individuals to demand compensation for violations. If there is no functioning compensation mechanism for these demands of individuals, effective protection of individual rights and freedoms is not feasible. The Court decision highlighting this situation holds great importance in this respect.

In the context of a different dispute referred to the Court of Justice of the European Union by the Austrian Supreme Court (C-487/21 – Österreichische Datenschutzbehörde/CRIF GmbH), the rights granted to the person concerned were subject to investigation. In the relevant decision, the scope of the data subject's right to request a copy of their personal data in pursuant to Article 15 f. 3 c. 1 of the EU General Data Protection Regulation was evaluated. This right, as being a matter of debate since the Regulation came into force, has been interpreted broadly by the Court. The Court ruled that the right to request a copy of the personal data subject to processing, if necessary for the data subject to exercise their rights, may also include the obligation to submit the relevant parts of the document or database containing such personal data or the entire document. Only in this case the individual will be able to effectively exercise their rights arising from the Regulation. Although the relevant decision introduces additional operational, financial and personnel obligations for data controllers, it is of great importance for individuals to use their rights arising from the Regulation in a functional manner.

Another important development related to the Austrian law concerns digital services offered by online platforms. Regarding the dispute in question, the Communication Platforms Act, enacted in Austria in 2020, imposes obligations such as reporting and appointing representatives on major social media platforms, and sets out penalties of up to millions of Euros in case of non-compliance. This provision is similar to the obligations imposed on social network providers under the Turkish Law No. 5651. Major platforms, including Google Ireland Limited, Meta Platforms Ireland Limited, and Tik Tok Technology Limited, argue that these provisions violate the country-of-origin principle adopted under Article 3 f. 2 of Electronic Commerce Directive 2000/31/EC. It is also argued that it is sufficient for these companies established in Ireland to comply with Irish laws, and that obligations such as appointing representatives and publishing reports in each Member State would violate the country-of-origin principle. Although a decision has not yet been made during the trial process, the prosecutor Szpunar presented his opinion under C-376/22 on 8 June 2023. In his opinion, Szpunar argued that the general-abstract acts enacted by Member States would be contrary to the provisions of Articles 3 f. 2 and 4 of Directive 2000/31/EC, if they affect the free movement of information society services, thereby favouring the platforms.

5.3. Ireland

As mentioned above, Ireland is the European headquarters of many technology companies due to its tax policies. Therefore, the global technology giants established their European headquarters in Ireland. Especially in data protection law, these enterprises are directly subject to the Irish Data Protection Authority. However, the Irish Data Protection Authority has faced criticism for its perceived 'tolerant' approach towards these enterprises. Although the highest fine imposed under the EU General Data Protection Regulation is the 1.2 billion Euros fine imposed against Meta by the Irish Data Protection Authority, the authority had to make this decision in response to the binding decision made by the European Data Protection Board.

The decision states that the personal data transfer made by Meta Ireland to Meta US are not in compliance with the conditions laid down in the GDPR for personal data transfer to third countries, hence, an administrative fine was imposed and additionally, a period of six months was given to the data controller to ensure that the data transfer is legal. The situation that constitutes unlawfulness is that Sec. 702 FISA and EO. 12333.70 and PPD-28, which are the basis of the PRISM and UPSTREAM programs implemented in the United States, do not provide sufficient protection regarding the processing of personal data obtained in the European Union. Although META has invoked the Standard Contractual Clauses (SCC) published by the Commission as the basis for personal data transferred to the USA, it has been determined that natural persons, whose personal data is processed, do not have the opportunity to seek rights similar to the Union standards before the US authorities, considering the right of access of the US authorities to such personal data.

The relevant decision is important both due to the amount of the fine imposed, but also due to the requirement to maintain the Union standards in third countries. In other words, the European Union aims to preserve the level of protection established within its own borders, even when the personal data of natural persons within the Union are processed outside its borders.

6. Comparison and Conclusion

In the digital age, the European Union began to take intensive regulatory actions to establish the general framework of the digital economy and to protect the fundamental rights and freedoms of individuals. These acts cover various areas such as personal data protection and privacy, electronic commerce and digital services, Internet law, cybersecurity law, competition law, artificial intelligence law, and product safety. Each legislative act introduces compliance obligations for EU Member States.

Although as a general trend for the Union previously preferred to prepare directives for the harmonisation of legislations and especially regarding the regulation of digital rights, the Union has recently began issuing regulations for this purpose. Therefore, the discretionary powers of Member States have become restricted, while unification is mostly achieved.

However, these legislative acts are not limited to imposing certain obligations on market actors. At the same time, many opportunities are offered to individuals in this regard. Within this framework, the Union has concluded that exclusive administrative penalties are quite insufficient, especially against large technology companies. Therefore, it is vital to establish and maintain functional mechanisms for individuals to claim their rights. Moreover, establishing and encouraging alternative dispute resolution mechanisms for disputes occurring in the digital space will contribute to the rapid resolution of disputes, and reduce the workload of the courts.

The legislative acts explained in detail above are also of great importance for administration. First, although unification is a matter of legislation, it will be inevitable to ensure coordination between Member States regarding the implementation of such legislation. Therefore, it is provided for that various new institutions will be established within the Union. The duty of these authorities is, rather than directly implementing regulations, to ensure coordination between the authorities of Member States, to ensure unification in practice, and to contribute to uniform implementation through guidelines, recommendations, and decisions.

Regarding positive aspects of the acts introduced in digital areas at the Union level, it would be useful to first discuss the legislative policy. As explained in detail above, various acts are envisaged to be enacted simultaneously in

many areas. It is of great importance that these acts do not conflict with each other. Subsequently, following the publishment of documents such as the European Union Digital Single Market Strategy, 2030 Digital Compass Communication, Digital Decade Policy Programme Decision and the European Declaration on Digital Rights and Principles for the Digital Decade, individual proposals for acts will be drafted accordingly. What is crucial regarding law-making techniques in digital areas is taking the information asymmetry between public authorities and market actors into consideration and subsequently preferring co-regulation methods instead of mandatory regulation techniques. In other words, in many acts in the digital field, a risk-based approach is assumed together with the principle of accountability, and the risk of engaging in unlawful and incompatible activities is transferred to actors who are in a more advantageous position in terms of information asymmetry. This approach is especially apparent in the administrative and technical measures that must be taken under the EU General Data Protection Regulation and in the quality management systems that are envisaged to be established under the Proposal for an Artificial Intelligence Act. Moreover, ensuring legal security through methods such as standards, certificates, codes of conduct and minimising compliance costs are another aspect of this approach. It is possible to see an example of this approach in the standards, certificates and codes of conduct laid down under the General Data Protection Regulation.

Another issue that is important in terms of regulatory logic relates to the flexible nature of acts. More specifically, given the developments in the digital field are very rapid, there will be a need to draft new legislative acts each time or to adapt the acts to these changes. Therefore, more flexible regulatory methods are preferred in Union acts. For example, the situations that require and do not require a data protection impact analysis under the EU General Data Protection Regulation are published by the European Commission in the form of white and black lists while lists of gatekeepers, who are described as very large online platforms under the Digital Markets Act, as well as high-risk AI systems in accordance with the Proposal for an Artificial Intelligence Act are also published by the Commission. What makes these lists non-exhaustible is that they are constantly updated by the Commission. Therefore, instead of a static act, a flexible one is provided for in the light of the technological developments and the resulting needs of change.

Regarding digital rights, the human-oriented approach of the EU is important. In other words, all technological developments carry substantial economic potential. However, this potential may also result in negative consequences. Lawmakers can eliminate the risk by completely prohibiting the new technology, but people will be deprived of all the benefits of technological advancements. On the other hand, not interfering with technology at all may cause irreparable harm, especially for individuals. The Union legislation, in pursuit of finding a balance between these two interests, aims to ensure the protection of the fundamental rights and freedoms of the individual at the highest level with a human-oriented approach.

Similarly, another issue that is important regarding the opportunities provided to individuals in the context of digital rights is the private enforcement approach. Accordingly, there are public institutions that supervise compliance with the law. Upon identifying illegal activities of market actors, these institutions can impose administrative fines, thus forcing these actors to act in compliance with the law. However, the only way to encourage market actors to comply with the law is not the penalties imposed by institutions. Besides, the imposed administrative fines correspond to a small portion of the revenues obtained by the relevant enterprises from their unlawful behaviour, and therefore cannot have a real deterrent effect. Therefore, individuals also have an important role in this. In other words, individuals can also force enterprises to act in compliance with the law both as part of their exercising their rights arising from the binding legislative acts of the Union, and especially within the framework of compensation claims. To this end, the existence of a functional mechanism in each Member State is critical. Moreover, violations, especially in the digital field, will most of the time not cause material damage to individuals or will only cause very minor damage. Therefore, there will mostly be claims for non-pecuniary damages. However, the uncertainty regarding the amount of non-pecuniary damages also causes many individuals to refrain from taking legal action against technology giants. Therefore, it is important to develop fast and easy alternative dispute resolution methods while providing for opportunities to file collective actions. As a concrete example of this, the EU General Data Protection Regulation lays down the possibility of filing a collective action by data protection associations and organisations.

However, these developments within the Union do not only have positive outcomes. The announcement of a new act every day entails significant compliance obligations and costs for market actors operating in the digital field. It will be inevitable for enterprises that want to operate in the digital field to consider the Union legislation as well as several national legislations. This situation, commonly referred as ‘overregulation’, gives rise to criticism within the Union that the freedom to conduct a business, provided for in Article 16 of the EU

Charter of Fundamental Rights, is disproportionately restricted.

When considering the impact of these acts in Member States, the economic and socio-cultural approaches of the Member States are worth mentioning.

For example, since data protection law in Germany has a long history, data protection authorities operate actively based on this rich experience. However, it should be emphasised that German data protection authorities often act in cooperation with data controllers, in other words, they apply the 'mandatory regulation' approach only in exceptional cases. Nevertheless, it should also be noted that due to the federal structure of Germany, there are issues that need to be taken into consideration on a state-by-state basis.

In the case of Austria, numerous issues are brought before the higher court, mostly owing to the efforts of data protection activist organization founded by Max Schrems. Therefore, although Austria ostensibly drawing less attention among the Union Member States in terms of population and corresponding economic volume, it is noteworthy highlighting that due to Austrian practice, many issues regarding the General Data Protection Regulation were brought to the higher court and these problems were clarified.

On the other hand, Ireland is a Member State that strives to attract technology giants due to low corporate taxes. Especially in the field of data protection law, the Irish authority has often faced criticism for not taking the necessary actions.

Therefore, although there is uniformity in terms of legislation, each Member State will not be prevented from developing a practice in line with its own interests. At this stage, Union institutions come to the stage and perform coordination duties to prevent different practices.

REFERENCES

Çekin MS, Berktaş AE, Akıncı MF, Veri Hukuku (On İki Levha Yayıncılık, 2023)

Develioğlu HM, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku (On İki Levha Yayıncılık, 2017)

Kama Işık S, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış (On İki Levha Yayıncılık, 2019)

Kuner C, Bygrave L A, Docksey C, The EU General Data Protection Regulation (GDPR) A commentary (Oxford University Press 2020)

Kühling J, Buchner B, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG (Beck, 2024)

Lambert PB, Understanding the New European Data Protection Rules (CRC Press - Taylor & Francis 2018)

Schulze R, Staudenmayer D, EU Digital Law - Article-by-Article Commentary (Nomos Verlagsgesellschaft 2020)

Taeger J, Gabel D, DSGVO BDSG TTDS (Deutscher Fachverlag, 2022)

Voigt P, Bussche A, The EU General Data Protection Regulation (GDPR) A Practical Guide (Springer 2017)

This project is funded by the European Union.

TÜRKİYE AND EU
FINANCIAL COOPERATION
FUNDAMENTAL RIGHTS

Technical Assistance for Strengthening Fundamental Rights Sector Coordination

CFCU
CENTRAL FINANCE & CONTRACTS UNIT

WEglobal