IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-05

INFORMATIONAL GOLD STANDARD AND DIGITAL TARE WEIGHT

– Country Report on Data Disclosure in the European Union

Prof Dr Kai von Lewinski

March 28th, 2022

Place of Publication

University of Passau IRDG
c/o Chair of German and European Private Law, Civil Procedure, and Legal Theory
Innstraße 39
94032 Passau

https://www.jura.uni-passau.de/irdg/

Abstract

This report was written within the framework of a comparative study from legal studies, cultural studies, and business informatics, which aims to investigate the extent to which decisions to disclose personal data are based on a cultural imprint as well as on the existing legal framework. In this report, we analyse and contextualise the functionalities and impact of data protection under the GDPR regime with a special focus on Germany. This includes German legal doctrine and relevant case law. To facilitate an overall assessment and comparison throughout the research project's eight country focusses, this report follows a matrix approach. This is, that it contemplates the rights and duties of the involved stakeholder groups (ie disclosure, recipient, organisations, regulatory authorities, public prosecution, judiciary, and legislature) in the legal fields (civil, public, and criminal law) and examines their respective means alongside the three levels of law (substantive, procedural, and enforcement law).

Cite as

von Lewinski, K. (2021). Informational Gold Standard and Digital Tare Weight – Country Report on Data Disclosure in the European Union. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-05*. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/

Keywords

Data Protection, Privacy, Country Report, Vectors of Data Disclosure, GDPR.

Contents

A. Generalities[1]

I. Cultural Vectors of Data Disclosure

(Identification of cultural [pre]conditions for individual data disclosure: cultural parameters that may the decision to disclose one's personal data; cultural practices and expectations regarding data disclosure [eg taboos]; data protection and privacy discourse, particularly articulated calls for reform); narratives and stories concerning data disclosure; synonyms for 'Data Protection' and 'Privacy' in the respective language.[2]

The EU member States certainly share **common 'occidental' values** (cf Art 2 of the TEU: 'The Union is founded on the values of (…)'). Regarding privacy, however, there are also considerable differences, even though following the GDPR data protection has (gained) substantial relevance in the EU.

See only – proverbially and as a stereotype – that there are no window curtains in the Calvinist Netherlands; that there is a general transparency concerning tax data in the Scandinavian countries; or that there are no 'residents' registration offices' in Ireland (nor in GB).

Most EU members States share a history of **experienced dictatorship and occupation** (fascist States, States of the Eastern bloc, occupation regimes).[3] Since the 1970s, there have also been changes in the relationship between freedom and security, especially in the context of terrorism (IRA, ETA, RAF, or Islamic terror).

European societies also share a **tradition of Statism** (except for Great Britain). This may result in a **low communitarian tendency** (except for Scandinavia and the UK) to share or donate data. Then again, there is **no firm culture of mistrust and secrecy (Arkan)** in Europe (this may be different in Eastern Europe?).

In many areas, European politics is characterised by an ideologically based stance. This self-conception as a '**moral role model**', especially regarding the colonial past, is in other parts of the world understood as cultural imperialism (this applies to the 'West' as a whole). Apart from the cultural aspect, this 'Brussels Effect' can also be understood as the European Union's self-confident stance in a data-economic and geopolitical context.

II. Legal System and Lawmaking

(central characteristics; sources of law and legal hierarchies; classification of legal systems); lawmakers and influential political and societal movements)

Fundamental to European Union law is the interplay between its **primacy of application and the EU's principal of conferral** by its member States. Accordingly, the EU is only competent to regulate in subject fields for which member States have explicitly transferred competencies in the 'treaties' (TEU, TFEU). In the field of information law, the EU's competencies are certainly far-reaching but not all-encompassing (the EU lacks competencies, eg, in the fields of the intelligence services, the military, the title system, and possibly disaster protection[4]).

---

[*] Professor Dr Kai von Lewinski is professor for Public Law, Media Law and Information Law at the University of Passau. The author wishes to thank the his research associate Sebastian J Kasper for translating this report's original German version into English which is available here.

[1] This report is part of an interdisciplinary research project on individual data disclosure: *Vectors of Data Disclosure – A comparative study on the disclosure of person-al data from the perspectives of legal, cultural studies, and business information systems research*, supported by the Bavarian Research Institute for Digital Transformation (bidt). <https://www.bidt.digital/en/vectors-data-disclosure/>.

[2] These guideline texts are meant to facilitate an overview on the structure and content of all of the research project's country reports.

[3] Cf Simson Garfinkel, *Database Nation* (2nd edn, O'Reilly & Associates 2001) 7, 14; differentiating Rudolph Houck, "'Common values" but not when it comes to data collection – differences in U.S. and German views on privacy' in Peter Dieners, Andreas Dietzel and Thomas Gasteyer (eds), *Liber Amicorum Dolf Weber* (Nomos 2016) 177 et seqq.

[4] Disputed by Gerrit Hornung and Jan-Philipp Stroscher, 'Datenschutz in der Katastrophe' [2021] GSZ 149–55; for a limitation of the powers of the

In the German and Romanic legal systems in continental Europe, there is a **culture of codification**, ie the tendency to collect law in more or less comprehensive codes. This aspiration to codify is difficult to achieve in the so-called multi-level structure of European and member State law; for multi-level codifications, ie a comprehensive European basic legal act with the member States' implementation, no convincing textual form has yet been found.

The **sources of law** are the European Treaties (TEU, TFEU, and CFR; so-called primary law) and a non-observable number of regulations, directives, and decisions (so-called secondary law) as well as implementing acts (tertiary law).

Whether the EU is now a separate **legal system** in the traditional sense of comparative law may be questioned. For (economic) administrative and regulatory law, it is acceptable to acknowledge an independent type of lawmaking. Both the common law (at least Ireland) and civil law (Roman law) are comprised as 'major legal systems' within the EU. A somewhat finer distinction – especially and traditionally for the civil law – can be made between the Roman-Germanic legal system (Germany and Austria as well as Greece, outside the EU also Switzerland, Liechtenstein, and Turkey), the Romanic legal system (above all France, but also Spain, Luxembourg, Belgium, in parts the Netherlands, and Portugal as well as Romania) and the Nordic legal system (Denmark, Sweden, Finland, outside the EU also Norway); it is questionable to what extent the post-socialist countries (still) form a separate legal system (called 'Eastern law'[5]).

European law is made through the **cooperation of the Commission, the Council, and the Parliament**; the respective procedure varies depending on the subject matter. The Commission is the (sole) initiator of legislation, the role of the (direct-elected but not representative-democratic) Parliament is relatively small. The Commission traditionally sees itself as the 'guardian of the treaties', the ECJ as the 'driver of integration', especially when interpreting the EU's competencies vis-à-vis the member States.

At the European Union level, those civic actors are influential that are also influential in the member States. Due to the EU's focus of competencies, **lobbying** in Brussels has a peculiar focus on economic and agricultural policy. - Whether Germany (as the largest and strongest member State) is stronger or weaker there, can hardly be answered unequivocally; after all, the EU is a post-war peace project (cf *Helmut Kohl*: 'Europe as a Question of War or Peace'[6]) to find a solution to Germany's geopolitically unfavourable size and location in Europe.

B. (General) Legal System of Information Law

I. Structure of Information Law

(constitutional and basic rights aspects; relevant regulations concerning intellectual property, secrecy, cybercrime [data privacy aut idem infra at C.]; Which regulations are based on international provisions [especially concerning intellectual property]?)

Due to the principle of conferral **there is no comprehensive regulatory competence for information law**. There is, however, a fairly far-reaching regulatory competence for intellectual property law (Art 118 of the TFEU) (which is, to a large extent, already harmonised globally) of which the EU has made ample use.[7] Currently, one focus of the

Union, see Kai von Lewinski, 'Art 1 DSGVO' in Martin Eßer, Philipp Kramer and Kai von Lewinski (eds), *DSGVO, BDSG und Nebengesetze* (7th edn, Heymanns C. 2020) para 22 (no longer held in the subsequent edition).

[5] Translated from German 'Ostrecht'.

[6] Translated from German 'Europa als Frage von Krieg und Frieden'.

[7] Kai von Lewinski, *Medienrecht* (C.H. Beck 2020) ch 8 paras 100–06.

EU's legislative activities is in the area of digital law, which, as far as the digital economy is concerned, falls within the core area of European regulatory competence for the European Single Market (DSA; DMA; DGA).

Due to the far-reaching exclusion of cultural matters from the EU's competencies (cf Art 167 of the TFEU), the EU's competencies in the cultural and also in the (journalistic-editorial) **media realm** are limited. Compared to older constitutional and human rights documents, the institutional importance of the media is explicitly recognised (Art 11(2) of the TFEU).

European constitutional law (primary law) gives **explicit recognition (including a regulatory mandate) for data protection** (Art 16 of the TFEU; Art 8 of the CFR). There is a more far-reaching regulatory competence for data protection law, because a reference to the European Single Market – that is usually required for European legislation – is not required (Art 16(2) of the TFEU). → see below B. II.

II. Allocation of Informational Legal Positions

(commodity/commoditization, especially 'intellectual property'; collective goods; public goods)

Intellectual property rights are generally recognised in accordance with international treaties (Berne Convention, etc.) (Art 118 of the TFEU; cf Art 36(1) of the TFEU: 'industrial and commercial property'). Public Sector Information (PSI) is subject of the Open Data and Public Sector Information Directive (EU) 2019/1024.

There is no right to personal data, but solely and instead a 'right to the protection of personal data concerning them' (Art 16(1) of the TFEU; Art 8(1) of the CFR). The Database Directive 96/6/EC does not protect personal data, but only an (ordered) database. And the Trade Secrets Directive (EU) 2016/943 at best creates a 'quasi-absolute' right to secrecy.

III. Institutions

(information supervisory authorities; private institutions/organisations [industry and sectoral associations], including international ones; public administration und cultivation/management of informational goods)

1. Supervisory Authorities

The European Commission is the central authority with comprehensive responsibility in the EU and is especially responsible for competition supervision. In addition, there are (an increasing number of) other authorities and agencies for specific matters. The European Intellectual Property Office [responsible, inter alia, for trade marks] (Alicante) should be mentioned in particular; the European Patent Office (Munich), however, is not an EU institution but is based on international law. There is no European media supervisory authority.

In terms of data protection, the European Data Protection Supervisor and the European Data Protection Board, both based in Brussels, should be mentioned. To date, the efficacy of supervision has not been definitively tested, particularly in the cross-border domain and vis-à-vis big data corporations.

2. Organisations/Associations

In keeping with its origins as the European Economic Community, industrial associations dominate around the European institutions. By now, many societal associations have become established as well. In the context of data protection, particular mention should be made of 'noyb' (none of your business), an activist organisation run by the Austrian *Maximilian Schrems*.

3. Public/States' Management of Information

No significant cultural organisations have been created at EU level – also because of the EU's limited competence in that field (Art 167 of the TFEU). The 'European' television channel ARTE is a Franco-German project on

a bilateral basis under international law. The (mostly public) cultural institutions in the European States belong to the member States.

Collecting societies for intellectual property are recognised by European law (Enforcement Directive 2004/48/EC).

IV. Procedural Aspects

(control and enforcement; individual; collective; through associations; by authorities [executive and judicial])

Europe and the EU are characterised by their developed liberal rule of law. The respective specific procedure is predominantly determined by the law of the member States. There is no individual complaint to the CJEU, but this is functionally compensated for by the opportunity to seek legal protection from the ECtHR (which is institutionally not part of the EU).

Following the environmental law model, collective legal enforcement mechanisms such as collective actions are becoming more widespread.

There are no special courts for information law issues; the 'Unified Patent Court' is not an EU institution but has a basis in international law.

In parts (eg in data protection) there is strong supervisory enforcement (→ see C. IV. 3. below).

C. Regulations Concerning Disclosure of Personal Data

I. Legal Structure of Data Disclosure

(existence of 'Data Protection Law'; mandatory and nonmandatory regulation; differentiation between public and private sector; public or private sector as a role model for regulation; general or sectoral regulation; self-regulation [codes of conduct]; basic principles of regulation [preventive ban or freedom of processing]; risk-based approach [potential for misuse; protection of certain categories of data]; privileged areas [personal and family sphere; media; research])

Data protection law is a category of EU law (with German roots[8]). This is because today's data protection law originated in Germany (in Hessen, to be precise), and then migrated up to the European level (also, but not solely, via other European States and to the Council of Europe [Data Protection Convention 108 of 1980]). Among other things, the (then) EC used this international convention as inspiration for a Data Protection Directive 95/46/EC. Following this directive, data protection laws in the member States have been revised (or have even been newly created). The GDPR then built on this first harmonization step.

In principle, EU data protection law cannot be derogated from, but in the relationship between the 'data controller' and the 'data subject' it can be shaped quite extensively by means of consent, although consent is itself quite presuppositional.

The distinction between the public and private (formerly: 'non-public') realms (which is significant at least in the German legal system) does not, at present, exist in European data protection law. With an expert eye trained on German data protection law, however, one can nevertheless recognise this dichotomous distinction in the scope exceptions of Art 23 of the GDPR and the JHA Directive.

The (German) data protection law originates from the scepticism towards State data processing (census, previously already microcensus and dragnet investigations), lesser and later also with regard to SCHUFA. European data protection law has concentrated on the economy because of its focus on the single market. The current debate on data protection and digital policy centres

[8] The fact that this German invention of data protection law had conceptual models (curiously enough) both in the USA (Miller, Packard) and (with regard to 'informational self-determination' in the (German Democratic Republic) GDR (!) should only be noted to complement the representation.

on the (US-American) digital corporations ('GAFA').

At the European level, the General Data Protection Regulation (GDPR) represents the approach of a general regulation; similarly, the JHA Directive, although it is sector specific as such, is a general regulation. For special areas of life and law, the telecommunications sector should be mentioned (E-Privacy Directive; planned E-Privacy Regulation).

Although (regulated) self-regulations (Artt 40 et seq of the GDPR) are regulated in detail, their practical significance is still very little.

The legal starting point of the GDPR is the prohibition unless permission is granted (cf the permissive elements in Art 6 of the GDPR). In addition, there are further rather organisational basic obligations (Art 5 of the GDPR).

There are only a few risk-based approaches in European data protection[9] (eg data protection impact assessment, mandatory appointment of a data protection officer; sensitive data). Even the exception for private-family activities is so narrow that even church choirs[10] fall within the scope of data protection law.

Despite its comprehensive regulatory concept, the GDPR is not applicable to all and everything. For example, it is limited by the scope of the EU's regulatory concept as a whole. Thus, parliamentary law (although this is disputed), pardon law, and title law fall within the member State's reserved realm. The applicability to health and disaster sectors is disputed. It also does not apply to the military (cf Art 39 of the TEU), nor to intelligence services. – Some subject fields are more or less excluded from the scope of the GDPR, such as the media (Art 85 of the GDPR) or access to information (Art 86 of the GDPR); in other fields, it leaves it open for Member States' regulations (such as employment, Art 88 of the GDPR; archives, historical research, and statistical purposes, Art 89 of the GDPR). In general, the GDPR's applicability is limited to electronic and (partially) automated data processing, excluding 'mental' or 'manual' data processing. In addition, private-family data processing (narrowly understood in practice) is excluded from the GDPR (Art 2(2)(c) of the GDPR, so-called 'household exemption'[11]).

II. Notions

1. (Personal) Data as Object of Protection

(situational [spoken words etc.]; local/spatial [at home]; logical ['spheres']; informational [datum, information]; treatment of public or publicized data; limitations and expansions of notions; categories)

The legal definition of 'personal data' in data protection law as the subject of protection under the GDPR is enshrined in Art 4(1) of the GDPR. It is understood broadly and also includes, in particular, the mere ability to relate data to persons.

Unlike the member States' legal systems which are, in this respect, rooted more deeply in history, European law – apart from the Charter of Fundamental Rights (Art 7 of the CFR) – does not provide any explicit protection for situational, spatial, or logical information and data protection.

Published personal data fall within the scope of the GDPR. In cases of journalistic-editorial publication or publications with the purposes of arts, literature, or expressing an opinion, they are referred back to member State law, Art 85 of the GDPR.

There are no restrictions or extensions at the factual level (such as legal fictions or presumptions).

---

[9] Decidedly different Markus Schröder, 'Der risikobasierte Ansatz' [2019] ZD 503–06.

[10] Case C-101/01 *Lindqvist* [2003] ECJ I-12971.

[11] Translated from German 'Haushaltsausnahme'.

Following the French legal tradition (and despite the general wisdom of data protection law stating that the context matters ['There is no such thing as a trivial date' and, conversely, none that is always relevant]), European data protection law recognises 'special categories of personal data' (Art 9 of the GDPR) as a type of data for which particularly high processing requirements apply.

The 'national identification number' (Art 87 of the GDPR) can also be considered a special type of data, or at least one that requires special regulation.

2. Allocation of Data to a Person

(creation; possession/control; personal connection; differentiation between domestic and foreign nationals; treatment of multi-referential data; limitations and expansions of notions; categories)

Data protection law assigns data to a person by means of a personal reference. The problem of the double reference of data (including the consequential question of the right of informational determination) is not addressed by the GDPR (and is still considered an unresolved issue).

Other means of assigning data can be found outside the realm of data protection law. For example in copyright law it is the act of intellectual creation that is relevant. For databases (although not the individual database entry) there is a separate European[12] intellectual property protection category: database law (Directive 96/9/EC). In the area of intellectual property rights, the focus is partly on the creation, and in the area of ownership and property rights, the focus is on the possession (eg of data carriers).

European law of personal data does not distinguish between nationals and non-nationals.

The dead are not considered persons and their data are not (any longer) considered personal; however, European law leaves room for Member States to supplement this rule.

For the 'special categories of personal data' it depends on whether qualifying characteristics exist in the person to whom the data relates. Neither the controller nor the place of processing or, in particular, the context are relevant.

3. Reception and Recipient

(special regulation for non-profit/non-commercial actors; the public as a [legal] recipient; use of public data; specialised/special obligations for small and medium-sizes enterprises (SMEs); differentiation between recipients and third parties [especially within company groups]; differentiation between national and international actions; outsourcing options)

The term 'recipient' is legally defined in Art 4(9) of the GDPR. In principle, the term is defined broadly. However, this provision provides for an exception for 'public authorities which may receive personal data in the framework of a particular inquiry [...]' (Art 4(9)(2) of the GDPR).

The public is not considered a recipient, but individual members of the public are.

Publicly accessible personal data can generally be processed under relaxed conditions; the balancing of interests as a general clause of (non-public) data processing then tends to favour the processor (cf also Sec 28(2)(1)(3) BDSG 1990).

In its basic conception, European data protection law does not follow a risk-based approach in which the size of the corporation would be a relevant parameter for the risk potential (rule-confirming exceptions are, however, eg Art 40(1) of the GDPR with recital 98, Art 42(1)(2) of the GDPR with recital 13; see also Art 37(1) of the GDPR), contrary to antitrust law (see its reliance on market power)[13].

[12] Internationally, however, this legal instrument could not be establish.

[13] On the question of whether antitrust standards are to be read into data protection law Boris Paal,

Data flows within a data controller did not constitute a transmission under conventional German data protection law. However, European data protection law now allows that the recipient does not have to be a third party, ie it can, e contrario, be part of the controller (disputed)[14].

The GDPR contains specific and detailed regulations for data transfers to third countries (Artt 44 et seqq of the GDPR).

One type of outsourcing is explicitly addressed in data protection law with the concept of processing ('Auftragsverarbeitung') (Artt 28 et seq of the GDPR). In addition, there was and still is the transfer of functions[15].

III. Relationship between Discloser and Recipient

1. Provisions for Disclosure

(Does regulation exist? personal data as intellectual property and commercial good; data law as a framework for action; 'informational self-determination')

'Data disclosure' is not a legal term in the GDPR, neither in relation to the data subject nor the controller.

Whether and under which conditions a data subject discloses personal data has always been regulated only indirectly in data protection law, namely in the form of consent, etc., which then forms an element of permission for (subsequent) processing by the controller.

Personal data are not intangible property, even if on a contractual basis (data licence agreement) they can be the subject of legal transactions. However, the often so-called 'dignity-based concept'[16] of European data protection law is categorically opposed to such commercialisation.

Nor does data law yet exist as a field of law that is understood in a broader sense. As an academic subfield, it is only just emerging.

Since 1983, 'informational self-determination'[17] has been almost synonymous with data protection in the German legal system; at least, according to the prevailing view, it is the constitutionally protected right (Art 2(1) in conjunction with Art 1(1) of the Basic Law). However, neither the concept nor the term 'informational self-determination' has been adopted outside Germany. From the general freedom of action (Art 2 (1) of the German Basic Law) and the general right of personality (Art 2 (1) in conjunction with Art 1 (1) of the German Basic Law), however, it is also possible to derive rights beyond data protection, some of which are older than modern data protection law; these include the right to one's own image (KUG, 'Kunsturheberrechtsgesetz', 'Copyright for Works of Art'), the right to one's own word and, in particular, the right to the written word.

a. Prohibited Disclosures

(protections of secrecy; multi-referentiality; disclosure to actors abroad; public communications)

For the individual, the principle of freedom of disclosure applies: I can disclose what I want, when I want, and how much I want[18]. Limits stem, however, from the rules on the

'Marktmacht im Daten(schutz)recht' [2020] ZWeR 215 et seq.

[14] Cf Martin Eßer, 'Art 4 DSGVO' in Martin Eßer, Philipp Kramer and Kai von Lewinski (eds), *DSGVO, BDSG und Nebengesetze* (7th edn, Heymanns C. 2020) para 91 with further proof.

[15] Comprehensive on this category adopted primarily in German data protection law: Thomas Petri, '§ 11 BDSG' in Spiros Simitis (ed), *Bundesdatenschutzgesetz* (8th edn, Nomos 2014) para 22 et seq; on its significance under European data protection law: Albert Ingold, 'Art 28 DSGVO' in Gernot Sydow (ed), *Europäische Datenschutzgrundverordnung Handkommentar* (2th edn, Nomos 2018) para 15 et seq.

[16] Translated from German 'würdebasierter Ansatz'.

[17] Translated from German 'informationelle Selbstbestimmung'.

[18] In a media law context on this Kai von Lewinski, *Medienrecht* (C.H. Beck 2020) ch 12.

protection of secrets, the impersonation or arrogation (of a public official)[19], and certain forms of depiction of one's sexuality[20]. In an economic context, the prohibition of misleading statements in competition law (UWG, 'law relating to unfair competition') draws further (and narrower) limits.

People can also communicate with and to the public as they wish within the general limits, and in doing so they can also disclose their data. The principle of freedom of media participation[21] applies as an expression of medial self-determination[22].

There are no specific regulations regarding disclosure abroad (except for constellations in spy novels).

The question of double- and multiple-referentiality of personal data is the great old and unsolved issue of data protection law. This is because it offers no practicable solution in cases in which, with regard to a date that refers equally to two persons (twins, spouses, etc.), one discloses it and the other does not.

b. Disclosure Obligations

(identification obligations and prohibition of anonymity; tax and other control)

Unlike in the Anglo-Saxon legal and cultural sphere, in (continental) Europe there is a fundamental registration of citizens and residents by the State; this is manifested in the residents' registration system and a fundamental obligation to provide identification. Thus, there is no fundamental right to anonymity (vis-à-vis the State), and 'identification procedures'[23] are not alien to the system.

In many cases, the controlling state also has the authority to request information from individuals (eg only in the context of pandemics, Sec 6 of the infection protection law 'IfSG'). However, as an infringement (of both freedom of action and informational self-determination) this requires a legal basis.

Apart from this, there is no general obligation to disclose or acknowledge information. This can be described as the right to 'informational self-preservation'[24]; this right derives from the general freedom of action in conjunction with, if necessary, Art 1(1) of the Basic Law.

c. Voluntary Disclosure/Voluntariness

(protection in dependency and hierarchy contexts; access to alternatives; prohibition of coupling; (voluntary) commercialization of personal data; incentives to data disclosure and protection therefrom [protection of adolescents; competition law; nudging]; prerequisites for consent; 'privacy fatigue'; peer pressure [eg WhatsApp])

Data protection law contains an explicit provision in Art 7(4) of the GDPR that contains standards for assessing sufficient voluntariness, which also includes the question of coupling. Current data protection law does not contain a categorical prohibition of coupling (Sec 28(3b) of the BDSG 2009 was stricter[25]).

A concretisation of the standards, especially regarding the availability of alternatives, is currently subject to legal proceedings. For example, the data protection activist group 'noyb' has tackled publishers and media providers for offering so-called 'pure subscriptions' for several euros per month as an alternative to consent-based user tracking.

---

[19] Kai von Lewinski, *Medienrecht* (C.H. Beck 2020) ch 12 para 55.

[20] ibid ch 12 paras 56–58.

[21] ibid ch 12.

[22] Gabriele Britz, *Freie Entfaltung durch Selbstdarstellung* (Mohr Siebeck 2007). Katrin Biermeier, *Mediale Selbstdarstellung* (Thesis at University of Passau, in preparation).

[23] Translated from German 'Erkennungsdienstliche Behandlung'.

[24] Translated from German 'informationelle Selbstbewahrung'. In a media law context, see only Kai von Lewinski, *Medienrecht* (C.H. Beck 2020) ch 13.

[25] Law from 14.08.2009, BGBl. I p. 2814.

Beyond data protection law as such, the law on general terms and conditions and competition law serve to protect consumers from overreaching by companies. Minors are specifically protected by the law for the protection of minors, especially from advertising. In labour law, criteria for protecting voluntariness have also been established for a long time; the best known is certainly the 'right to lie' when asked about pregnancy, and the most recent issue concerns the vaccination status.

The approach in data protection law that used to be more firmly followed – namely, to increase the consent's warning function but also to make it unattractive (especially in the internet context) through (written) form requirements (cf Sec 4a(1)(3) and (4) of the BDSG 2001) – no longer exists in today's data protection law (cf Art 7 of the GDPR).

Peer pressure regarding consent is not reflected by law, except for the indirect consideration of market position in antitrust law[26].

2. Recipient's Obligations

a. Requirements for Personal Data Reception

(information; requirements concerning content and formalities; warnings; notifications; assurances)

Although 'recipients' are legally defined in the GDPR (Art 4(9) of the GDPR) they are not norm addressees[27]. In this respect, the normative programme under data protection law applies merely and only when received personal data is processed by it (and the 'recipient' thereby becomes the 'controller' as defined by Art 4(7) of the GDPR).

In addition to the general obligations (Art 5 of the GDPR) and the requirement to dispose of a legal basis (Art 6 of the GDPR), the processor is subject to information obligations (Artt 12 et seqq of the GDPR).

b. (Procedural) Obligations Concerning Received Personal Data

(purpose dedication/limitation; technological and organisational measures; data security; deletion and retention; further transmission and limitations thereto, also concerning transmission abroad)

Received data that is processed within the meaning of the GDPR (cf Art 4(2) of the GDPR) must comply with the general principles for processing (Art 5 of the GDPR) and those of the specific permitting clause (Art 6 of the GDPR).

3. Control by Discloser

a. Transparency and Right to Request Information

In addition to (and due to) the transparency provisions (Artt 12–14 of the GDPR), the data subject has a right to information (Art 15 of the GDPR).

Beyond data protection law, labour law (in particular regarding the content of the personnel file) and health law (regarding the medical file and diagnostic findings) provide for a comprehensive right to information.

In media law, there is even a special regime of not having to provide information about sources.

b. Co-Determination and Co-Decision Concerning Data Use

(restrictions for use; reservation of consent; revocation of consent; contestation and objection; special rules for international contexts; technical requirements for the act of permission/consent)

In data protection law, in the narrow sense, data subjects have a right to 'rectification' (Art 16 of the GDPR), a right to 'erasure' (Art 17 of the GDPR; in certain aspects politically communicated as the 'right to be forgotten' [Art 17(2) of the GDPR]) and a right to 'restriction of processing' (Art 18 of

[26] On this: protection law Boris Paal, 'Marktmacht im Daten(schutz)recht' [2020] ZWeR 215 et seq.

[27] No provision of the GDPR determines a legal consequence for recipients.

the GDPR; formerly in the BDSG 'blocking'[28]).

The data subject can also raise an 'objection' (Art 21 of the GDPR). If data processing is legitimised by consent, this can be 'withdrawn' (Art 7(3) of the GDPR. The 'objection' also plays a role[29] in the context of the balancing of interests (Art 6(1)(f) of the GDPR).

For international transmissions, no additional or special subject rights apply; however, the enforceability of data protection options is a criterion for assessing the lawfulness of a transmission abroad (cf Art 46(3)(b) of the GDPR).

In accordance with the technology-neutral regulatory approach of the GDPR, there are generally no technical requirements for cooperation. A rule confirming the exception may be seen in Article 7(3)(4) of the GDPR, which stipulates that the withdrawal of consent should not be more difficult than the consent itself.

c. Revocation

(Data portability; deletion; 'right to be forgotten / to forget')

While the possibility to withdraw consent (Art 7(3) of the GDPR) only legally eliminates consent, but it remains possible to base data processing on another legal basis, data protection law also establishes original data-related claims: On the one hand, there is the (systematically quite controversial) right to data portability (Art 20 of the GDPR). On the other hand, there is a right to 'erasure' under Art 17 of the GDPR with the iteration of Art 17(2) of the GDPR ('right to be forgotten')[30].

The 'right to forget' does, among others, not apply in the media sector (Art 17(3)(a) of the GDPR; unless already exempted under Art 85 of the GDPR). In this context, the German Federal Constitutional Court has through its case law (and certainly on a European [fundamental] law basis) established specific standards with the 'right to be forgotten'[31].

Apart from that, the disclosure of data is an actual act (like revealing secrets) that, de facto, cannot be 'put back in the bottle'.

d. Procedural Aspects

(costs for and effectivity of the rights of the affected persons [information, etc]; consumer appropriateness)

The exercise of data subject rights under the GDPR is generally free of charge (Art 12(5)(2) of the GDPR; cf also the argument e contrario from Art 15(3)(2) of the GDPR). The costs of exercising the rights (→ see C. III. 4. on enforcement below) are (initially) borne by the party invoking them in accordance with the general principles of procedural law.

If one turns to data protection authorities (Art 77 of the GDPR) – the same applies to consumer and data protection associations (Art 80 of the GDPR) – exercising data subject rights is free of charge entirely; due to the procedural discretion of the authority and the private autonomy of the associations, the data subject then has no further controlling possibilities.

4. Enforcement

a. Damages and Compensation

([material and immaterial] damages; reparations; disgorgement of profits; punitive damages)

Under data protection law, data subjects who have suffered material or non-material damage because of a data protection breach can claim compensations for such damage (Art 82 of the GDPR). The exact requirements and, in particular, the assessment of the damage and the compensations to be awarded are currently being debated in the courts.

---

[28] Translated from German 'Sperrung'.

[29] Naming according to Kai von Lewinski, Giselher Rüpke and Jens Eckhardt, *Datenschutzrecht* (C.H. Beck 2018) paras 25, 177 et seqq.

[30] Case C-131/12 *Google Spain* [2014] ECJ I-317.

[31] BVerfG. Judgement of 06 November 2020. *Recht auf Vergessen I* – 1 BvR 16/13.; BVerfG. Judgement of 06 November 2020. *Recht auf Vergessen II* – 1 BvR 276/17.

Outside of data protection law, under general tort criteria, it is not sufficient for a violation of a data protection regulation, but only a violation of a (personality) right in order to claim damages on the basis of Sec 823(1) of the German Civil Code (Bürgerliches Gesetzbuch, BGB).

In media and celebrity law, there is also the figure of unjust enrichment in the amount of fictitious licence fees, etc., which, however, presupposes an already existing commercialisation and thus a market price.

Punitive damages are not known in data protection law and especially not in German tort law. (A similar disciplinary effect, however, may have the German specific of the warning letter; → see C III 4. b. below)

b. Procedural Aspects

('threshold' for legal protection; right to initiation; burden of proof and evidentiary privileges; dispute value; 'small claims'; alternative dispute resolution; rights to bring/press charges; 'rational apathy')

The data subject must enforce his or her data protection and other rights him or herself and also bear the costs and cost risks. This is done through normal court proceedings; there is no special data protection procedural law.

However, one can also 'make use' of the data protection authorities to enforce rights by complaining to them (Art 77 of the GDPR). The data protection authorities are not, however, a will-less tool in the hands of the data subject but have procedural discretion (both in terms of the 'whether' and the 'how'). The data subject can only force a complaint to be addressed by means of a petition-like procedural remedy (Art 78(2) of the GDPR).

A German specificity are competition law warnings, according to which competitors as well as competition and consumer associations can claim an injunction against an infringer. Applying the rules of 'agency without specific authorisation' (Secs 677 et seqq of the German Civil Code, BGB), the infringer has to bear the (procedural) costs for this. Above all, it is the enormous speed (within 24 hours or less) that makes the warning letter a very effective means of enforcement.

IV. Objective Legal Obligations of the Recipient

1. Obligations Concerning Received Data

a. Dependence on Authorisation

(of business models, processing variants, terms and conditions)

Data protection law does not contain any authorisation requirements. – In general, data protection law has a very strong focus on the specific processing step which would be unsuitable for an authorisation concept at today's computing speed. Thus, business models, procedures, and also general terms and conditions (privacy policies) need not and cannot be submitted for approval (unlike, for example, under Sec 10 of the Federal Data Protection Act, BDSG, in its former version); contractual clauses and other guarantees for international data transfers (Artt 45 and 46(2) of the GDPR) or of codes of conduct under Artt 40 et seq of the GDPR are exceptions confirming the rule (see also in summary Art 58(3) of the GDPR).

Beyond data protection law, there are rules in antitrust law according to which certain business models which then also manifest themselves in procedures (including general terms and conditions) require approval or, in any case, the competition authorities have the power to participate and exert influence.

b. Notification Obligations

(regarding business models and business activities; regarding processing activities)

Similar to what applies to authorisation (→ see C. IV. 1. a. above), there are no notification duties under data protection law.

c. Documentation

(accountability)

A comprehensive documentation obligation exists in data protection law in the form of accountability in Art 5(2) of the GDPR.

Beyond data protection law, there are retention and documentation obligations in various contexts (for example in tax, commercial, and accounting law). Where they do not exist, they are regularly useful for any subsequent legal defence.

d. Processing Requirements

(prohibition subject to permission; balancing of interests; restrictions for terms and conditions; business practices; APIs/interfaces for third parties)

In accordance with its nature as a general regulation, the GDPR does not provide for specific processing requirements. However, as a result of the prohibition of processing subject to permission (Art 6 of the GDPR) the processing conditions must be based on the (admittedly very abstract) requirements of Art 6 of the GDPR. There, the balancing of interests (Art 6(1)(f) of the GDPR) is particularly important.

Beyond data protection law and oriented rather to the role of the consumer than the data subject under data protection law, the law on general terms and conditions also sets out requirements for contractually agreed processing conditions.

Moreover, if companies (outwardly) engage in business practices they are liable for their compliance according to the law relating to unfair competition's (UWG) rules for misleading.

Specifications for technical interfaces exist but once in general data protection law (Art 20(1) of the GDPR: 'commonly used [...] format'). In telecommunications (data protection) law, there are specifications for interception interfaces (Sec 170 of the Telecommunications Act 2021 [TKG 2021]; formerly Sec 110 of the Telecommunications Act [TKG]).

e. Prohibitions and Obligations

(prohibition of processing variants [eg profiling]; criminal prohibitions; restrictions under competition regulations; prohibition of abuses [of power/market power]; further transmission to third parties, especially governmental bodies; elicitation from abroad)

Beyond what is described above, data protection law does not operate with legal prohibitions – probably because of the general (preventive) prohibition subject to permission (cf Art 6 of the GDPR). An (apparent?) exception is Art 22 of the GDPR regarding automated individual decision-making.

2. Monitoring

a. Recipient's Self-Monitoring

(self-restrictions; compliance mechanisms; internal responsibilities [company privacy officers; ombudspersons)

According to the general criteria, compliance with laws is incumbent upon the (respective) norm addressee. In principle, it is then also up to him in which way s/he wants to comply with the laws (as long as s/he complies). Data protection law, however, in its role as an anticipatory protection, imposes a number of precautions on the controller that are intended to (additionally) ensure compliance with the data protection rules. This includes the accountability (Art 5(2) of the GDPR), which not only focusses on the success of compliance with the law but also ensures that all the controller's actions are directed towards compliance and that the legal situation is reflected.

Furthermore, a data protection officer must be appointed, both in a private company and a public authority (subject to a threshold to be set by the member States, Artt 37 et seqq of the GDPR). This is a special hybrid between an internal expert within the organisation and an ombudsperson.

Beyond the requirements of data protection law there are corporate law and other compliance requirements and voluntary commitments.

b. Regulated Self-Regulation

(sectoral and industry associations)

The GDPR contains a detailed set of rules for regulated self-regulation in the form of 'codes of conduct' (Artt 40 et seq of the GDPR). In practice, this institute has not had much effect so far.

Depending on the business sector, there are numerous sectoral rules outside of data protection law.

c. Supervisory Authorities

(data protection authorities; competition authorities; economic oversight authorities)

Data protection supervision rests with the data protection authorities regulated in detail in the GDPR (Art 51 of the GDPR). They are independent in a very specific way (determined by European law).

As with any administrative competence, there may be overlaps with other authorities' competencies, be it with those for consumer protection, general security and public order authorities (including the police) or – most recently and particularly relevant – the competition authorities.

d. (Specific) Criminal Prosecution

(focus) prosecution units for informational offences; [situational/special] investigators)

In terms of the number of cases, data protection criminal law has hardly played a significant role. Even under the GDPR, as far as can be seen, there has not been a significant increase in investigations and convictions. Consequently, it is not surprising that (in Germany) the prosecution of data protection offences is handled by the general criminal prosecution authorities.

Special investigators are not known to exist; however, the data protection authorities may transmit the (initial) suspicion of a criminal offence to the competent prosecution authority.

e. Procedural Aspects

(investigation powers; resources of monitoring institutions)

Data protection authorities have extensive and wide-ranging investigative powers (Art 58(1) of the GDPR). What limits their efficacy is their relative size and equipment compared to the importance of personal data processing in developed post-industrial societies. There are also differences between the authorities in Germany (which are multiplied due to Germany's federal structure) and those in some other EU Member States[32].

3. Enforcement

a. Interventions Concerning Data Processing

(restriction and prohibition of data processing)

The data protection authorities have far-reaching and numerous powers of intervention (Art 58(2) of the GDPR) which primarily relate to specific processing and, in addition, to technical and organisational deficiencies.

b. Interventions Concerning Business Models

(competition and economic supervision; government/public monopolies)

Contrary to antitrust and competition law and financial services supervision, there are no business model-related powers of intervention (cf Art 58(2)(f) of the GDPR: 'limitation […] on processing').

c. Sanctions for Processors/Processor-related Sanctions

(prohibition orders concerning business activities; corporate sanctions; revenue-based sanctions)

[32] With special reference to the Irish data protection supervisory authority which is key to the control of the US digital corporations: Bastian Benrath and Hendrick Kafsack, 'Datenschutzwüste Irland' *FAZ* (Frankfurt, 13 September 2021) also with comparative figures for other EU States.

The legal consequences that may follow (continued) data protection violations are listed exhaustively in Art 58(2) of the GDPR.

Fines regularly affect the controller, which is usually not a sole trader or partnership, but a legal entity.

The amount of a fine relates to the (worldwide) annual revenues.

d. Sanctions for Individual Actors

([managing] directors' liability; individual criminal sanctions)

Liability of the managing director is not excluded under the general regulations (compliance liability, liability under employment law or law applicable to civil servants and public officials[33] of the [company's or authority's] data protection officer, possibly also tort liability under Sec 823(1) and/or (2) of the German Civil Code, BGB).

e. Procedural Aspects

(priority of data regulation enforcement; resources of enforcers; shaming impact/pillorying effect of breaches/violations)

The provability of data protection violations is facilitated by the existing accountability – otherwise there is in any case a violation of accountability...

Due to the low threshold for data protection violations and the low infringement of legal interests (compared to offences against violation of personal life and secrecy, Sec 201 et seqq of the German Criminal Code, StGB), the data protection offences (of which only few are reported; → see C. IV. 2. d. above) are not prosecuted as a matter of priority.

The data protection authorities are well equipped; however, they are sometimes considered to be understaffed. By contrast, the general criminal prosecution authorities have a sufficiently large apparatus for the prosecution of data protection offences.

The pillorying (or shaming) effect of data protection violations, at least for companies that participate in the consumer market, is great. Often, the damage to a company's image caused by data protection proceedings is considered greater than the sanction that is later imposed.

D. Sources and Literature

I. Related Monographs

Marion Albers and Ingo Wolfgang Sarlet (eds), *Personality and Data Protection Rights on the Internet* (Springer 2022)

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition#publication-tab-0> accessed 22 March 2022

Christopher Kuner, Lee A Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Nikolaus Marsch, *Das Europäische Datenschutzgrundrecht* (Mohr Siebeck 2018)

Kai von Lewinski, Giselher Rüpke and Jens Eckhardt, *Datenschutzrecht* (2nd edn, C.H.Beck 2022)

Indra Spiecker gen. Döhmann and others, *General Data Protection Regulation* (Nomos/Hart 2022)

II. Related Articles

Marco Bassini, 'Fundamental rights and private enforcement in the digital age' [2019] 25(2) European Law Journal 182

Raphaël Gellert, 'Understanding the notion of risk in the General Data Protection Regulation' [2018] 34(2) Computer Law & Security Review 279

Christoph Krönke, 'Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt

[33] Translated from German 'Dienstrecht'.

am Beispiel der Datenschutz-Grundverordnung' [2016] 55(3) Der Staat 319

Henry Pearce, 'Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protectin Rights under EU Law' [2018] 4 European Data Protection Law Review 190

Paul Quinn and Gianclaudio Malgieri, 'The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework' [2021] 22(8) German Law Journal 1583

III. Leading Cases

Case C-131/12 *Google Spain* [2014] ECJ I-317.

BVerfG Judgement of 06 November 2020. *Recht auf Vergessen I* – 1 BvR 16/13.

BVerfG Judgement of 06 November 2020. *Recht auf Vergessen II* – 1 BvR 276/17.

BVerfG Judgement of 15 December 2009. *Vorratsdatenspeicherung* – 1 BvR 586/08.

IV. Miscellaneous

Kai von Lewinski, *Die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes* (Mohr Siebeck 2014)