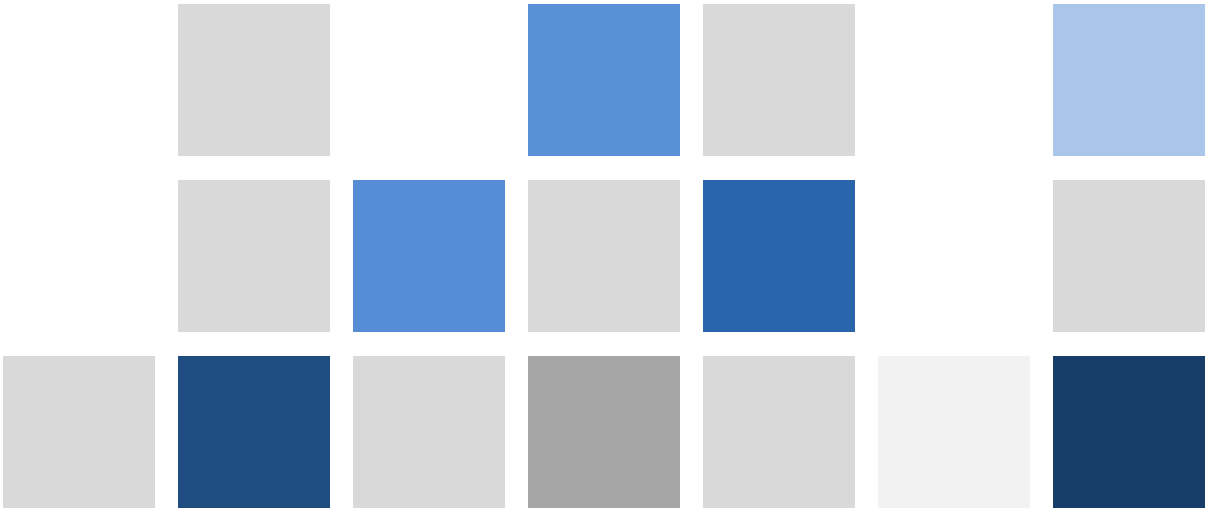
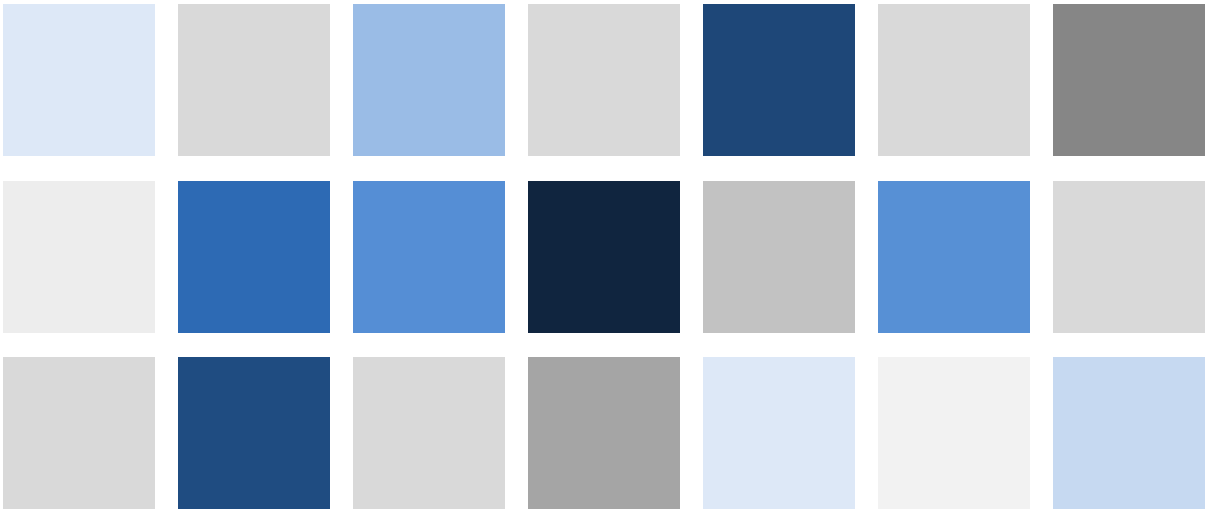


Long-term data for Europe

EURHISFIRM

3.2: Report on the Legal Issues Related to the Protection of Privacy and Personal Data



This project has received funding from
the European Union's Horizon 2020 research and innovation programme
under grant agreement N° 777489

AUTHOR(S):
Helmut Siekmann
(JOHANN-WOLFGANG-GOETHE-UNIVERSITÄT FRANKFURT AM MAIN)

APPROVED IN 2021 BY:

Jan Annaert (Universiteit Antwerpen)

Wolfgang König (Goethe Universität Frankfurt)

Angelo Riva (École d'Économie de Paris)

Table of Contents

The Report on Work Package 3.1 (WP 3.1) mainly covers intellectual property rights issues and topics from competition law whereas this Report relates to Work Package 3.2 (WP 3.2) and deals with ethics, which is mainly understood as the legal rules protecting privacy and personality rights and partially extended to (sub-legislative) legal norms and by-laws.

To the extent possible, the report will refer to the source materials presented in "D4.2: Report on the Inventory of Data and Sources" and examine whether and if so which rights might be affected by the materials. It will furthermore examine whether the possible utilisations of the materials in the context of the database project might infringe those rights or whether they fall within the scope of a limitation of, or an exception from, these rights.

1. Introduction

The ultimate goal of the EURHISFIRM project is to create a database for long-term firm data from six different Member States of the EU (Belgium, France, Germany, the Netherlands, Poland and Spain), and a former Member State, the United Kingdom of Great Britain and Northern Ireland. An essential part of the creation of such a database is the collection and processing of data and historical sources containing such data.

The legal and ethical questions arising from such an undertaking touch upon distinctively different fields of the law. This is why Work Package 3 (WP 3) was divided into two parts that were treated consecutively:

- Task 3.1: Open access: Ownership and property rights of data and sources
- Task 3.2: Data privacy and information protection.

Due to this separation of the tasks, the work also results in separate reports: the Report on Intellectual Property Rights Related Issues and Topics from competition law by *Alexander Peukert* (D3.1) and the Report on Ethics (Privacy and Information Protection Issues, Constraints and Solutions) by *Helmut Siekmann* (D3.2). In the second report the ethical challenges are considered.

At least on the Continent, it has for centuries been a generally accepted fact that a legal norm differs categorically from other types of norms or just "normal" behaviour which might develop prescriptive power. Since (only) legal norms that are derived from the law of nations, the law of the EU and of the various states (including the UK) may be imposed on non-consenting persons, they will govern the work of EURHISFIRM with binding force. They have to be the "centre of gravity" for both academic treatment and practical governance. Commandments from moral philosophy or religion can only be binding for a believer. Since the Enlightenment, they have belonged to the domain of philosophers and theologians but not of lawyers. The report on WP 3.2 is, therefore, focussed on the legal protection of personal data and privacy by the primary and secondary law of the EU.

In view of the growing encroachment of governments on dissenting individuals in the vicinity of the EU or even within the Union and in view of the amassing of (vital) data by private corporations and institutions increased emphasis is being placed on the protection of privacy. It has to be respected,

regardless of whether it is enacted in a strict legal norm. The notion of privacy and of personal data has extensively been elaborated by the Court of Justice of the European Union.[1] The leading cases are *Digital Rights Ireland*,[2] *Schrems I*,[3] *Tele2 Sverige*,[4] and *Schrems II*[5]. Previously several seminal judgments were handed down by the German Federal Constitutional Court (GFCC – *BVerfG*).[6] The jurisprudence of the European Court of Human Rights (ECtHR) has to be taken into account as well.[7]

1.1. Objectives of this Report

Following the latest developments in the European legislation on data protection in response to the jurisprudence of the Court of Justice of the EU, WP 3.2 mainly analyses legal issues such as (data) privacy that will arise during the design and the implementation of the research infrastructure. It results in some practical guidelines.

A closely related but separate issue is the protection of the (personal) data processed by EURHISFIRM against interior or exterior infringements. This has to be distinguished from the privacy issues which are touched on in the *due course* of the instalment and working of EURHISFIRM. The goal of data protection is to shield these data from *irregular* actions while they are in the domain of the Research Infrastructure. It ought to be named "data security". Privacy can only be provided if the security of data is guaranteed.

In this context, special attention needs to be paid to processing and sharing personal or person-related data *without explicit consent* and for *other purposes* than those for which they were originally collected. This will be the case for the overwhelming part of the information processed by EURHISFIRM.

(1) Guideline for EURHISFIRM

Data protection and data security should be distinguished.

1.2. Organisation of the Report on WP3.2

The Report is organised as follows: It begins with a discussion of the ambiguous meaning of the term "ethics" and its role in a legal context (2.), followed by an overview of the relevant sources of law (3.). A crucial point for EURHISFIRM is the discussion of the overarching principle that data protection is confined to the protection of natural persons (4.). Then the Primary Law of the EU is inspected (5.). Turning to the secondary law of the EU, a specific emphasis is laid on the General Data Protection Regulation (GDPR), which has become the predominant legal source for judging all data protection-related issues (6.). Some specific problems, including the protection of the data of deceased persons,

[1] For a comprehensive discussion see *M.Brkan,* German Law Journal (2019), 864-883.
[2] Joined Cases 293 & 594/12 of 8/4/2014, *Digital Rights Ireland v Minister for Commc'n*, ECLI:EU:C:2014:238.
[3] C-362/14 of 6/10/2015, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, [*Schrems I*].
[4] C-203/15 of 21/12/2016, *Tele2 Sverige* (meta-data retention).
[5] C-311/18 of 16/07/2020, *Data Protection Commissioner, Facebook Ireland Ltd, Maximilian Schrems*, ECLI:EU:C:2020:559 [*Schrems II*].
[6] BVerfGE 65, 1 (informational self-determination – judgment on census); 100, 313; 115, 166 (online search); 120, 274 (protection of information technology); 120, 351, 128, 1; 133, 277.
[7] See e.g. ECtHR of 13/9/2018, Application Nos 58170/13, 62322/14, 24960/15.

which is highly relevant for EURHISFIRM, are revisited and the "codes of conduct" are treated in more depth in the final part of the Report (7.).

2. Ethics in a Legal Context

The term "ethical" in the description of the objectives of WP 3 is taken up from the overarching title of WP 3: "Legal and Ethical Design". This wording necessitates some explanatory reflections.

2.1. Morality and Legality

For a long time in history, there was no clear distinction between ethical and legal norms. They blended into each other or were seen as identical. Often not even an adequate terminology had been developed to enable a distinction. In some parts of the world this is still the case – with growing tendency. It was, however, one of the great achievements of the Enlightenment in the Western world to dissolve the confusion between morality[8] and legality. From the 16th century on, this brought tremendous progress in the organisation of societies so as to promote individual welfare and to protect life, liberty and estate of all human beings, granting them unalienable rights as individuals.[9] The collectivistic approach, cultivated by many beliefs and almost all authoritarian or totalitarian regimes, was overcome. Each individual was considered to be a value in itself, first in theoretical thinking and then increasingly over time in the practical design of states and their constitutions.[10] It was basically legal structures, like the written catalogues of fundamental or civil rights and institutional provisions (e.g. sovereignty of the people, separation of powers control by an independent judiciary) that both promoted and shielded this development.[11] Human dignity reached the summit of all rights and values.[12] It was also a regime change for the endeavours of science and technology, thus enabling the sustainment of many more people in the first place and eventually a much longer life in comfort and in some parts of the world in peace.

After the Reformation ethical beliefs became too heterogeneous to continue to serve as a generally accepted source for binding rules. The discord resulted in some of the bloodiest wars in history,[13] first in England and then on the Continent. Eventually, all attempts to derive (binding) legal norms from principles of moral philosophy bluntly failed, mainly because their content was and is *arbitrary,* at least on concrete problems. Law-making might not be completely isolated from some very basic requirements of moral philosophy but the *application* of the law definitely is and has to be kept strictly separate from ethical or moral considerations, considering the diversity and (contradicting) plurality

[8] The precise demarcation between ethics and morality is unclear. Often they are used synonymously; see *Esser* in his profound treatise (Grundbegriffe, 1949, page 25); also a recent publication: *Möllers*, Legal Methods, 2020, page 39 footnote 34, with further references. But it is also claimed that a precise distinction is essential, whereby morality is to be lodged on an operative level, as it refers directly to the acts which are considered to be good or bad in a society, whereas ethics must be lodged on a meta-level: cf. *Schulze,* Die Sünde, 2008, p. 247; referring to *Pieper,* Einführung, 1994.

[9] *Kriele*, in: Festschrift Stern, 1991, page 15-23.

[10] *Welzel*, Naturrecht, 1962, pages 139 et seq.

[11] For a detailed description of the development see *Stern*, Der Staat des Grundgesetzes, 1992, pages 997-1023 (first published 1984); *ibid*. Staatsrecht I, 1984, pages 63-65, 93-95; *ibid.*, Staatsrecht III/1, 1988, pages 64-94.

[12] *Stern,* Staatsrecht III/1, 1988, pages 13-23.

[13] *Welzel*, Naturrecht, 1962, pages 110 et seq.

of "ethical" demands.[14] "Ethical" norms are more or less created at will and are *not consistent* through times.[15] Good examples are the prosecution (and ultimately killing) of "witches" or "infidels" as an ethical obligation or – changing the perspective – the condemnation of same sex relationships and – only a few decades later – the reverse condemnation of anybody who dares to criticize same sex marriages.

The heterogeneity of such norms and their time-inconsistency disqualifies them also as a general source to fill blanket clauses referring to e.g. the public good or common decency (*gute Sitten*)[16] like in Sections 138 and 826 of the German Civil Code. A legal action is judged in this context as an infringement (*sittenwidrig*) if it "contravenes the sense of decency of all just and equitable thinkers" (*verletzt das Anstandsgefühl aller billig und gerecht Denkenden*), or more idiomatic: if it violates the ethical feelings of all just and fair thinking. Since this definition does not contain much substance, ethics and morality or other non-legal, generally accepted customs might indirectly morph into binding norms, but only as rare exceptions and usually with the caveat that morality in this context does not mean ethics in the sense of moral philosophy or religious belief.[17]

Most important in a democratic state is, however, that the creation of such "ethical" rules lacks the benefits of the moderation of its contents by an open discussion in a predefined legislative procedure and the protection of fundamental rights. Often they are considered not to be created but revealed from a transcendental (or "divine") source and thus not debatable. These are the main reasons why such rules must not be enforced on the general public, even if individual followers might treat them as binding, often trying to impose them on non-believers via the sovereign powers of the government. They have to remain in the private domain of the believers.

2.2. Replacement of the transcendental sources of law

After the loss of a generally accepted transcendental source of legitimacy for the rules governing life in a state and society,[18] tradition (often in the form of the monarch) served in some countries as a substitute, especially in Central and Eastern Europe. In the more advanced North-Atlantic states, namely in the British colonies on the North American continent,[19] the people was "invented" as the

[14] See *Dreier,* in: Gedächtnisschrift für Theo Mayer-Maly, 2001, page 157; *Möllers,* Legal Methods, 2020, page 46 et seq.

[15] See *v. Münch,* in: Festschrift Klaus Stern, 1997, pages 49 (52, 55).

[16] See e.g. the comprehensive treatments by: *Mayer-Maly,* Archiv für Civilistische Praxis (AcP) 194 (1994), pages 105 et seq.; *Dreier,* in: Gedächtnisschrift für Theo Mayer-Maly, 2001, pages 141 et seq.

[17] This is indispensable in view of the utilization of the clause by the judiciary to infiltrate the civil law codifications with the Nazi idealogy when deemed useful, see RGZ 150, 1 (4) (*"herrschendes Volksempfinden, die nationalsozialistische Weltanschauung*"). In favour of strict prohibition of any recourse to "ethical norms" irrespective of its kind or guise: *Schachtschneider,* Festschrift für Werner Thieme, 1993 195 et seq.; in effect similar *Dreier,* in: Gedächtnisschrift für Theo Mayer-Maly, 2001, page 157; dissenting with a total prohibition but in general also restrictive *Mayer-Maly,* Archiv für Civilistische Praxis (AcP) 194 (1994), page 106, 171 et seq., 174 et seq, but in general ; dissenting BGHZ 17, 327 (332), shortly after WW II, at a time when the Court still tried to overcome the schools of thought which allegedly lead to the atrocities of the "Third Reich" by integrating to a large extent roman-catholic dogmas into its case law.

[18] Rationalism, science and natural law were for many the driving force, see e.g. *Welzel,* Naturrecht, 1962, pages 110, 112, 139 et seq.

[19] *Stern*, Der Staat des Grundgesetzes, 1992, pages 997-1023 (first published 1984); *Kriele*, in: Festschrift Stern, 1991, pages 20 (France), 23 (British colonies in North America).

sole source of legitimacy for exerting sovereign powers.[20] Even if the founding fathers were in their majority good Christian believers and often referred in their writings to the Bible, the people replaced transcendental or ethical systems as the basis and source for all worldly government. Now the motto was: government of the people, by the people, for the people. The republican form of government with sovereignty vested in the people could no longer derive its legitimation from a moral-philosophical entity as before (*dei gratiae*).

This meant not only an emancipation from the traditional sovereigns but from ethical systems as well. The freedom of religion and its free exercise attributed as a birth-right to each human being became one of the main driving forces for establishing individual rights – enforceable in court – and state-neutrality with the separation of legal systems from the (ethical) norms taught by religious beliefs or similar convictions (*Weltanschauungen*). The separation is clearly expressed in Article 1 of the French Constitution: *La France est une République indivisible, laïque, démocratique et sociale*. The East and Central European states, however, lagged far behind this development for a long time, partly well into the 20th century, like Germany.

From this follows that ethical norms not only lost their overcome legitimation but, that they lack *any* legitimation for binding someone who is not a believer, unless they are transposed into a legal norm enacted in the due democratic process combined with minority rights. Just like an ethical rule, such a norm must not be imposed on somebody else who might adhere to a different ethical system or – as an agnostic – may not adhere to one at all. To a limited extent they might be rendered binding if they are accepted by contractual consent. But such a contract would have to be subject to judicial control. It has to be kept in mind that it is also a fundamental right not to believe and to be left alone by any missionary approaches.

The utmost a legal system can demand of citizens is that they abide by the law. In principle, it cannot demand that they follow certain ethical categories, which in a modern state have to be a strictly private matter. Morality and Legality have to be clearly separated.[21]

In addition, ethical categories fall into the domain of philosophers or theologians and not of lawyers. Hence, considerations of moral philosophy cannot be the subject of this report.

(2) Guideline for EURHISFIRM

Ethical rules can only be binding for an individual or group of individuals who believe in them, and they must not be enforced by state powers. With limits, they might be binding if (voluntarily) accepted on

[20] *Morgan,* Inventing the people, 1988.

[21] *Hart,* Concept of Law, 1961 (1970), page 181: "though this proposition [that a legal system *must* exhibit some specific conformity with morality or justice, or *must* rest on a widely diffused conviction that there is a moral ogligtion to obey it] may, in some sense, be true, it does not follow from it that the criteria of legal validity of particular laws used in a legal system must include, tacitly if not explicitly, a reference to morality or justice"; see also *v. Münch,* in: Festschrift Klaus Stern, 1997, page 52, having been both an academic scholar and a member of a state government; partially disagreeing *Esser,* Grundbegriffe, 1949, page 25 et seq.

a contractual basis but subject to judicial control and the essence of fundamental rights protecting non-believers.

2.3. Ambiguous Meaning of the Terms "Ethics" and "Ethical"

The delineations between ethics and law are, however, blurred by the growing influence of the thinking and terminology of the English-speaking world in supranational organisations and in the non-English-speaking world in general. The terms "ethics", "ethical" and "unethical" became virtually inflationary in 20th-century politics and media but without sufficiently considering that these words have a significantly broader meaning in the English-speaking world. From there, they gradually also crept into the legal language, usually in legal argumentation of persons without a formal legal education or when promoting a specific agenda that is not part of the legal system; sometimes under the veil of "codes of conduct", which have become quite popular too.

As outlined above, outside the English-speaking world the terms "ethics", "ethical" and "unethical" were eradicated from law and legal thinking and reserved to Philosophy and Theology. In the English language, however, they are not necessarily understood as categories of moral philosophy or of *Weltanschauungen.* They can also have a much wider meaning in the sense of by-laws, statutes of self-governing bodies, or generally accepted customs in closed entities. In the light of this understanding they largely denote legal norms and not categories of moral philosophy, but of a lower rank in the hierarchy of norms. They may play a certain role in the interpretation and application of ambiguous terms in legal norms but have no binding force on courts of law. One of the reasons for this divergence is the initial lack of codifications and the dominating role of judge-made law (case law) in the common law systems with the consequence that there did not develop such a clear delineation between the making of the law and the application of law as on the continent.

With their dispersion into media and politics, the terms "ethics", "ethical" and "unethical" lost their originally – well-defined – meaning. Good language and precise terminology is usually not the hallmark of politics and media. In addition, another imminent danger is threatening: These terms are increasingly employed as tools to promote special interests which could not or did not achieve the necessary majorities in the due course of (democratic) legislation. In conjunction with the practice of capturing the (public law) media, financed by contributions, minorities and losers in parliamentary vote can impose their objectives and convictions (*Weltanschauungen*) on others as if they were very binding (legal) norms, simply by naming a desired conduct as "ethical" and shaming the opposite as "unethical". In effect the beneficial separation and moderation of powers and the requirements of a due process set up for good reasons can be circumvented or altogether levered out. In fact, with the help of media they act as prosecutor, judge and executor in one without any chance of a proper judicial review.

2.4. A Generally Accepted Minimum?

As outlined above, a modern state must not demand that its members act in conformity with the rules of a more or less arbitrary moral philosophy. Even if this principle is relaxed for the most basic ethical requirements, like "respect your fellow human being" and "do not inflict harm on your neighbour" they do not have any practical significance since they are everywhere part of the legal system, at least

in the Western world.[22] Caveats and relativisations of these extremely abstract rules in concrete conflicts, like "without (just) cause" are highly controversial and have to be resolved anyhow by the legal system. Torturing or even killing a heretic in an open street is widely considered to be a just cause for the deviation from the generaly accepted minimum within certain ethical systems; this even in an – allegedly – Western society. That makes the (too) general rules almost meaningless for practical purposes.

This holds true especially for the subject matter of this work package, the protection of privacy and personal data by the EU and its Member States. By now both areas have been regulated in a density that leaves no room for "ethical" considerations in the narrow sense of the word.

(3) Guideline for EURHISFIRM

Ethical rules in the genuine sense of the world must not play a significant rule in the context of EURHISFIRM.

This insight should not be questioned by the observations made by philosophers advocating re-moralisation: In the course of the 20th century, moral condemnation for acts done in private and the concept of sin almost completely disappeared in the Western world. In sum, this century brought a "negation of the morally dressed-up domestication of the subject". Everything goes from the perspective of philosophy.[23] However, a "re-moralisation" can – allegedly – be observed in the last two decades, now not (external) requirements based on holy revelations but as obligations of the *forum internum* to do good on oneself.[24] On the other hand, the step from holy to secular ethics brought a growing uncertainty about the contents and a tremendously increasing abstractness of the generally accepted rules.[25] The result is the arbitrariness of the ad-hoc guidelines in codes of conducts or the like and the possible necessity of developing ethics as a discourse on ethical rules on a meta-level which is named *Transzendentalpragmatik*.[26]

2.5. Directives and Guidelines of the EU

Directives of the EU are indisputably legal norms addressed at the Member States (Article 288(3) TFEU).[27] "Guidelines" are in principle non-binding if they are issued by an institution of the EU as recommendation or opinion. Article 288(4) TFEU orders explicitly that they shall have *no binding force*.

[22] *Hart* calls those very obvious generalizations "truisms", Concept of Law, 1961 (1970), page 188: "Such rules do in fact constitute a common element in the law and conventional morality of all societies which have progressen to the point where these are distinguished as different forms of social control"; unfolding further the complex relationship betwee laws and morality but always coming to the point that a distinction between the two is inevitable (page 207).

[23] *Schulze,* Die Sünde, 2008, p. 243 ["In der Summe war das 20. Jahrhundert eine Negation der moralisch verbrämten Domestikation des Subjekts."]

[24] *Ibid.,* p. 245.

[25] *Ibid.,* p. 249, 251

[26] *Ibid.,* p. 251, footnote 27; referring to *Hösle,* Krise der Gegenwart, 1994, p. 109 ff.; critical in view of filling gaps or reversing statutary decisions *Mayer-Maly,* Archiv für Civilistische Praxis (AcP) 194 (1994), pages 175 et seq.

[27] Treaty on the Functioning of the European Union, Consolidated Version. Official Journal of the European Union of 7 June 2016, C 202/1.

Notwithstanding, a host of guidelines and recommendations has been issued by the European Data Protection Board[28] and may be used in the interpretation and application of legal norms as described in Section 2(2.5).

(4) Guideline for EURHISFIRM

"Ethical" norms in the sense of technical standards or (generally accepted) best practices might exert some indirect force by guiding the interpretation and application of open and vague terms in legal norms. Under these conditions and with these restrictions "ethical" norms might have (very limited) binding force for the design and work of EURHISFIRM.

2.6. Conclusion

The concrete description of tasks 3.1 and 3.2 demonstrate that the emphasis of Work Package 3 has to be on legal questions. The term "ethics" mainly serves as a bracket between the legal fields of privacy protection and information protection (intellectual property). Both fields have to be distinguished precisely but are not completely isolated from each other. They may intersect at certain points but differ in substance.[29]

Privacy is closely tied to the core of a natural person's personality and its protection by the (general) personality right[30] whereas the protection of information (in general) can serve to protect privacy but need not necessarily do so. Often it refers to (confidential) business data without a link to the privacy of a human being. To a large extent such information is covered by intellectual property rights, but it may exceed them substantially.

Ethical questions in the strict sense of the word might be touched on when interpreting and applying legal norms.[31] Whenever this happens, a clear demarcation is, however, indispensable and it has to be always made absolutely clear that it is a legal norm which is interpreted and applied. The legal norm has to be the justification and basis for every sovereign act, even if the separating line is quite often erroneously blurred by interested stakeholders from non-legal fields who in the public debate allege that ethical norms they attempt to promote can have universal binding force regardless of a foundation in law.

Because of the wider connotation of the term "ethics" in the English-speaking world[32] quite frequently *legal* norms of a lower rank, like by-laws, administrative orders, charters (of self-governing bodies), articles of incorporation, or administrative regulations and provisions are meant. "Codes of Conduct" for certain professions are sometimes designated as "ethical" norms. Under certain preconditions they might be binding (legal) norms, though always subject to the requirements of democratic

[28] See Section 6(6.2)(6.2.3) infra.
[29] *v. Münch,* in: Festschrift Klaus Stern, 1997, page 49 (52, 54, 61).
[30] BVerfGE 120, 180 (199); 120, 274 (311).
[31] *Möllers,* Legal Methods, 2020, page 471, but somewhat critical about the strict separation between lawmaking and the application of law (against the prevailing view) page 77 et seq., with further references.
[32] See Section 2.3 above.

legitimation.[33] Generally accepted principles, usually technical standards for the practical work of engineers or craftspersons, might also be denoted as "ethical" rules in the English-speaking world. Whether they can have binding force is questionable.[34] Their domain is the interpretation and application of vague and open terminology in a legal norm, like "processed fairly" and "legitimate basis" in Article 8(2) Charter of Fundamental Rights of the European Union (CFR) or "legitimate interests" in Article 6(1) lit. f GDPR.

At least the General Data Protection Regulation (GDPR)[35] is based on an understanding of the term "ethics" as (legal) rules governing the conduct of "regulated professions".[36] This understanding is also obligatory for the "Codes of Conduct" extensively regulated by Chapter IV, Section 5 of the GDPR.

As these may be organised in totally different ways in the EU Member States, no general overview is possible.

(5) Guideline for EURHISFIRM

The "ethical" design of EURHISFIRM must be restricted to the obedience to legal norms. It may, however, encompass (i) "codes of conduct" for specific professions and (ii) technical standards or best practice rules.

3. Relevant Sources of Law

Unwritten legal rules derived from common law or customary law have to be considered in theory but for all practical purposes have disappeared on the continent to almost non-existence.[37] At least they do not play a significant role in the protection of privacy and personal data. The vast majority of the relevant rules are derived from written statutes. In any case they prevail since they contain codifications. Thus, the report has to focus on them.

[33] With good reasons restrictive *Sachs,* in: Sachs (ed.), Article 20 margin numbers 44 et seq.; somewhat more lenient: BVerfGE 10, 89; 15, 235; 37, 1; 38, 281; however demanding at least the possibility of a final parliamentary control: BVerfGE 135, 155 margin number 156 et seq; 136, 194 margin number 68 et seq.

[34] See for this debate *Möllers,* Legal Methods, 2020, pages 46, 77-79, in specific margin numbers 7 and 8, demonstrating the exceptions which are all highly questionable from a systematic approach.

[35] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016; corrected by: Corrigendum to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 127/2, 23.5.2018 – consolidated version: https://eur-lex.europa.eu/eli/reg/2016/679/OJ/eng.

[36] See e.g. the wording in Recital 73 GDPR: "breaches of ethics for regulated professions".

[37] Against the existence of such law *T. Möllers,* Legal Methods, 2020, page 85 at margin number 29,, at least as far as it touches on fundamental rights.

3.1. European Convention for the Protection of Human Rights and Fundamental Freedoms

The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[38] is a legal source which might in view of its subject matter be a relevant source of law for the establishment and operation of EURHISFIRM. Article 8(1) of the Convention protects the right to respect for private and family life.

The Convention was enacted as a separate legal instrument by the Council of Europe at Rome on 4 November 1950.[39] It is not an (integral) part of the EU law but the EU has finally acceded to it,[40] fulfilling its obligation from Article 6(2) TEU[41] in the version of the Treaty of Lisbon[42] and overcoming all (prior) legal concern. Beforehand, it had already been ratified by all Member States of the EU including the UK.

The right of Article 8(1) ECHR is, however, granted only subject to exceptions (Article 8(2) ECHR) such as interference of public authority in accordance with the law and is necessary in a democratic society in the interest of a variety of objectives:

---

[38] See for the full original text: https://www.echr.coe.int/Documents/Archives_1950_Convention_ENG.pdf; see for the consolidated (up-to-date) text: https://www.echr.coe.int/Documents/Convention_ENG.pdf.

[39] Entering into force in 1953.

[40] Protocol (No 8) relating to Article 6(2) of the Treaty on European Union on the Accession of the Union to the European Convention on the Protection of Human Rights and Fundamental Freedoms, OJ C 306/155, 17.12.2007; published again in conjunction with the Consolidated Versions of the Treaty on the European Union and the Treaty on the Functioning of the European Union, OJ C 202/01/273, 7.6.2016.
Declaration on Article 6(2) of the Treaty on European Union, OJ C 306/249, 17.12.2007; published again in conjunction with the Consolidated Versions of the Treaty on the European Union and the Treaty on the Functioning of the European Union, OJ C 202/01/337, 7.6.2016:

> The Conference agrees that the Union's accession to the European Convention for the Protection of Human Rights and Fundamental Freedoms should be arranged in such a way as to preserve the specific features of Union law. In this connection, the Conference notes the existence of a regular dialogue between the Court of Justice of the European Union and the European Court of Human Rights; such dialogue could be reinforced when the Union accedes to that Convention.

[41] Its full wording is:

> The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.

Protocol (No 8) relating to Article 6(2) of the Treaty on European Union on the Accession of the Union to the European Convention on the Protection of Human Rights and Fundamental Freedoms, OJ C 306/155, 17.12.2007; published again in conjunction with the Consolidated Versions of the Treaty on the European Union and the Treaty on the Functioning of the European Union, OJ C 202/01/273, 7.6.2016.
Declaration on Article 6(2) of the Treaty on European Union, OJ C 306/249, 17.12.2007; published again in conjunction with the Consolidated Versions of the Treaty on the European Union and the Treaty on the Functioning of the European Union, OJ C 202/01/337, 7.6.2016:

> The Conference agrees that the Union's accession to the European Convention for the Protection of Human Rights and Fundamental Freedoms should be arranged in such a way as to preserve the specific features of Union law. In this connection, the Conference notes the existence of a regular dialogue between the Court of Justice of the European Union and the European Court of Human Rights; such dialogue could be reinforced when the Union accedes to that Convention.

[42] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community signed at Lisbon, 13 December 2007 (OJ C 306/1, 17.12.2007); entry into force on 1.12.2009, https://www.europarl.europa.eu/factsheets/en/sheet/5/the-treaty-of-lisbon.

- national security,
- public safety,
- economic well-being of the country,
- prevention of disorder or crime,
- protection of health or morals,
- protection of the rights and freedoms of others.

Altogether they cover such a wide scope of topics and goals that it is safe to assume, for all practical purposes, that the ensuing highly specified legislation is in compliance with these requirements.

Irrespective of the precise legal character of the Convention, in concrete cases, Article 8 ECHR might serve as a guidance for interpretation and an acknowledgement of the fact that privacy is an object of legal protection by its being granted as a fundamental right. Most important is, however, that the European Court of Human Rights consistently refused in its case law the application of Article 8 ECHR on the protection of deceased persons.[43]

(6) Guideline for EURHISFIRM

In essence, it should be derived from Article 8 ECHR that privacy is in principle protected as a human right but is, in principle, confined to living persons.

3.2. Law of the European Union

To a large extent, the data protection law is harmonised within the EU. Therefore, the relevant sources of law are mainly the *primary* and *secondary law of the EU* including the decisions and judgments of the *Court of Justice* of the European Union (CJEU).[44] This is crucial for judging the protection of privacy and personal data in the context of EURHISFIRM.

(7) Guideline for EURHISFIRM

The relevant legal rules for the protection of privacy and personal data are harmonised within the EU. In subject matters, the national law of Member States is limited to a marginal role.

3.2.1. Primary Law

Altogether the primary law contains three provisions regulating the protection of privacy and personal data.[45]

[43] *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 233; see for more details Section 7(7.1)(7.1.3).
[44] For reasons of simplicity the report only refers to the CJEU, even though some of the judgements referred to were made at a time when the Court was generally referred to as the European Court of Justice (ECJ [*EuGH*]).
[45] See also *M. Schröder,* in: Streinz, EUV/AEV, Artikel 16 AEUV margin number 1.

a) *Charter of Fundamental Rights of the European Union*

Privacy is expressly protected by Article 7, and personal data by Article 8 of the *Charter of Fundamental Rights of the European Union* (CFR). The Charter enshrines certain political, social, and economic rights for European Union (EU) citizens and residents. Article 47 CFR covering judicial rights might also be relevant. However, limitations are permissible under certain prerequisites (Article 52(1) and (2)) but have to leave the essence of the rights untouched. With justification they may be infringed but a mass surveillance would unlawfully compromise the essence of the right.[46]

The Charter was drafted by the European Convention and solemnly proclaimed on 7 December 2000 by the European Parliament, the Council of Ministers and the European Commission. Its then legal status was uncertain and it did not have full legal effect[47] until the entering into force of the Treaty of Lisbon on 1 December 2009.[48] Since the ratification of that Treaty it has full legal effect as part of EU law (Article 6(1) TEU).[49] Its consolidated full wording has been published in the Official Journal of the EU.[50]

A debated question was whether and to what extent the human rights regulation is binding for the Member States. Article 51(1) CFR provides that the provisions of the Charter are addressed to the institutions and bodies of the Union only when they are implementing Union law. This way the concerns of some Member States, especially of the UK, were mitigated that the Charter would extend additional new EU law into them. This limitation notwithstanding, the human rights regulation binds the Member States (i) indirectly whenever provisions of the Treaties have to be interpreted, (ii) when individual rights are granted but subject to national derogation and (iii) when they implement EU rules.[51]

From this follows that the Charter has been given the "same legal value as the EU Treaties".[52]

b) *The Treaties*

Another principal legal source of the primary law of the EU for assessing the protection of personal data is Article 16 of the Treaty on the Functioning of the European Union (TFEU). Article 16(1) TFEU

---

[46] CJEU case C-362/14 *Schrems I,* at margin number 94; critical in view of the criterion: access to content *M. Brkan,* 14 Eur. Const. Law Review, pages 360 et seq., 368.

[47] Even more restrictive *T.C. Hartley,* Foundations, 2014, chapter 5 § 2.3: "no legal force".

[48] For reference to the Treaty see footnote 42.

[49] Declaration concerning the Charter of Fundamental Rights of the European Union, OJ C 306/249, 17.12.2007; published again in conjunction with the Consolidated Versions of the Treaty on the European Union and the Treaty on the Functioning of the European Union, OJ C 202/01/337, 7.6.2016:

> The Charter of Fundamental Rights of the European Union, which has legally binding force, confirms the fundamental rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States.
>
> The Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined by the Treaties.

[50] See OJ C 202/389, 7.6.2016; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016P/TXT

[51] *Ibid*., at § 2.4.

[52] *Hartley*, Foundations, 2014, chapter 5 § 2.3.

and Article 8(1) CFR may be treated simultaneously, since the crucial general principle is identical: Every individual has the right to the protection of personal data concerning her or him.

Article 39 of the Treaty on European Union (TEU) also refers to the protection of personal data. In substance it orders that the Council, by way of derogation from the general rules of the encompassing paragraph 2 of Article 16 TFEU, shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data. This obligation is, however, confined to activities of the Member States within the scope of Chapter 2 of Title V TFEU containing specific provisions on the common foreign and security policy of the Union. Hence, it is of no relevance for EURHISFIRM.

c) Conflict of Laws

In theory, the existence of two human rights codices in Europe could create problems since the Convention "goes beyond" the Charter "in a number of ways".[53] Article 52(3) of the Charter provides, however, a rule to solve possible frictions: This rule makes clear that in case the Convention and the Charter cover the same rights, the provision of the Convention precedes in the interpretation and scope of the ECtHR, established on the basis of the Convention. This way the judgments of this Court are also authoritative for the interpretation and application of rights of the Charter. From this follows that Articles 7 and 8 CFR have to be applied according to the judicature of the ECtHR.[54] This is higly relevant for EURHISFIRM.

The second sentence of Article 52(3) ECHR, however, provides an opening for Union law to go further and provide a protection beyond the provisions of the ECHR. This clause also allows the CJEU to pursue a wider interpretation than the ECtHR.[55]

In case the EU Treaties themselves contain provisions for the protection of a specific human right, Article 52(2) CFR provides that rights recognised by the Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties. The result would be precedence of the provisions in the Treaties over provisions of the Charter. Since Article 8(1) CFR and Article 16(1) TFEU are identical save the variation in the – legally meaningless – attempt at gender-correct language the question is of no practical significance.

3.2.2. Secondary Law

The main source for rules on the protection of privacy and personal data are the provisions of *secondary law*; foremost the General Data Protection Regulation (GDPR).[56] The instruments of secondary law also contain some guidelines for procuring data security and data safety.

[53] *Hartley*, Foundations, 2014, chapter 5 § 2.3; *Brkan,* German Law Journal (2019), 20, Page 870 et seq.
[54] Consenting but with reservations *M. Brkan,* German Law Journal (2019), 20, Page 870, presenting as an example of discord: ECtHR Application Nos 58170/13, 62322/14, 24960/15 of 13/9/2018, *Big Brother Watch v United Kingdom*, paras 224-28, 463, and CJEU C-203/15 of 21/12/2016, *Tele2 Sverige*, ECLI:EU:C:2016:970.
[55] *Hartley*, Foundations, 2014, chapter 5 § 2.3.
[56] See for reference footnote 35.

a) General Data Protection Regulation

The GDPR, which entered into force on 25 May 2016, creates a harmonised set of detailed rules applicable to personal data processing taking place in the EU.[57] It is applicable from 25 May 2018 (Article 99(2) GDPR).

The GDPR builds on the fundamental rights and expressly confirms in its Article 1(2) that the protection of natural persons in relation to the processing of personal data is a "fundamental right". In addition, it also refers in its motives to Article 8(1) CFR (the "Charter") and Article 16(1) TFEU providing that everyone has the right to the protection of personal data concerning him or her.[58]

b) Regulation on Data Processing by EU Institutions

The Regulation on Data Processing by EU Institutions (IDPR),[59] created two years after the GDPR, lays down specific data protection rules which apply (only) to EU institutions, bodies, offices and agencies. It was created in 2018 and has to be applied from 12 December 2019 on. Like the GDPR it refers to the fundamental rights and reiterates that the protection of natural persons in relation to the processing of personal data is a fundamental right. It also builds on Article 8(1) CFR and Article 16(1) TFEU. Moreover, it restates that the right to the protection of personal data is also guaranteed under Article 8 of the Convention.[60]

Although the GDPR provided already for the adaptation of Regulation (EC) No 45/2001 on the processing of personal data by EU institutions in order to ensure a strong and coherent data protection framework in the Union and to allow its application parallel with it, the EU thought it necessary to pass a new regulation covering the topics of Regulation 45/2001 in order to "align as far as possible the data protection rules the data protection rules for Union institutions, bodies, offices and agencies with the data protection rules adopted for the public sector in the Member States".[61]

The provisions of this regulation follow to a wide extent the same principles as the provisions of the GDPR. At its initiation it was expected that those two sets of provisions should, under the case law of the CJEU, be interpreted homogeneously, in particular because the scheme of this regulation should be understood as equivalent to the scheme of the GDPR.

At least at the moment, EURHISFIRM cannot be considered to be a Union institution or body. This implies that it is not covered by the IDPR. In case this changes in the future, a comprehensive treatment of details is not required because of the mainly identical treatment of the relevant rules in both regulations. Only if substantial material differences show up will a more in-depth treatment be advisable.

---

[57] See *European Data Protection Board,* Legal framework, https://edpb.europa.eu/legal-framework_en.
[58] Recital 1 GDPR.
[59] REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295/39, 21.11.2018.
[60] Recital 1 IDPR.
[61] Recital 5 IDPR.

The separate Data Protection Regulation for EU Institutions (IDPR), created two years later, has to be observed from December 2019 on.

c) Law Enforcement Directive

The Law Enforcement Directive (LED) was adopted together with the GDPR on 27 April 2016,[62] and entered into force on 5 May 2016 (17 May 2016). It is addressed to the Member States (Article 65 LED), and had to be transposed into the EU Member States' legislation to be fully applicable by 6 May 2018 (Article 63(1) LED).[63] The scope of this Directive is limited to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, pursuant to Article 2(1) in conjunction with Article 1(1) DPD.

Due to its special scope the LED will not be relevant for EURHISFIRM and needs no further treatment here.

d) Electronic Communication Privacy Directive

The Directive on privacy and electronic communication from 2002 (ePrivacy directive) is still in force.[64] It is *lex specialis*[65] in view of the GDPR which in effect does not impose additional requirements on the electronic communication (Article 95 GDPR)[66] which covers in principle - but not only - all internet traffic.

The attempts to renovate the ePrivacy directive and adopt a new regulation[67] parallel to and harmonized with the GDPR had failed for a long time despite the need to do so.[68] At the beginning of

[62] DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89, 4.5.2016.

[63] This way, Member States were granted sufficient time to implement the new rules in their national law, which had to be accomplished by 6 May 2018; see *European Data Protection Board,* Legal framework, https://edpb.europa.eu/legal-framework_en.

[64] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ, 31/7/2002, L 201/37; amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11) (Directive 2002/58).

[65] Recital 173 GDPR.

[66] "This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC."

[67] Now: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) of 10.1.2017, COM(2017) 10 final. 2017/0003 (COD)

[68] Recital 173 GDPR: "In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation." For further details see *Klabunde/Selmayr*, in: Ehmann/Selmayr, 2018, Article 95 margin number 22.

2021 at least a consensus within the Council has been reached giving the Commission a mandate for negotiations with the Parliament for the final wording.[69] The draft ePrivacy regulation will repeal the existing ePrivacy directive. As *lex specialis* to the general data protection regulation (GDPR), it will particularise and complement the GDPR. For example, in contrast to the GDPR, many ePrivacy provisions will apply to both natural and legal persons.[70]

The Directive is mainly addressed to the providers of the infrastructure for electronic communication and of access to these services. Its material scope is confined to the "provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices"

Hence, it is of only little relevance for the core activities of EURHISFIRM.[71]

e) European Electronic Communication Code

The European Electronic Communication Code from 2018[72] is a directive to create "a legal framework to ensure freedom to provide electronic communications networks and services, subject only to the conditions laid down in this Directive and to any restrictions in accordance with Article 52(1) of the Treaty on the Functioning of the European Union (TFEU), in particular measures regarding public policy, public security and public health, and consistent with Article 52(1) of the Charter of Fundamental Rights of the European Union". It is "part of a 'Regulatory Fitness' (REFIT) exercise, the scope of which includes four Directives, namely 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC, and Regulation (EC) No 1211/2009 of the European Parliament and of the Council".[73] Although it also refers to the ePrivacy directive as being "part of the existing regulatory framework for electronic communications networks and services,"[74] it did not repeal or recast it like the other legal acts mentioned.

Similar to the ePrivacy directive, it is "applicable to providers of electronic communications networks and of electronic communications services" and recasts "the four Directives in order to simplify the current structure with a view to reinforcing its consistency and accessibility in relation to the REFIT objective" and adapts their "structure to the new market reality, where the provision of communications services is no longer necessarily bundled to the provision of a network".[75] Therefore, it is only of marginal relevance for EURHISFIRM. The protection of privacy and personal data is not its relevant subject matter and objective.[76]

---

[69] Press release of 10 February 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/.
[70] *Ibid*.
[71] See for more details Section 0(7.4)(7.4.1).
[72] DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code (Recast), OJ, 17/12/2018, L 321/36.
[73] *Ibid.,* recital 4.
[74] *Ibid.,* recital 2.
[75] *Ibid.,* recital 4.
[76] See for more details Section 0(7.4)(7.4.1).

f) Safe Harbour Agreement

A heavily criticised legal act of the EU serving as source of law was the *informal agreement* between the EU Commission and the US Government on handling the data protection and privacy issues ("Safe Harbour Agreement"). Its conformity with superior law and its binding force were heatedly debated. Finally, the CJEU struck it down in its judgment of 6 October 2015.[77]

The ensuing replacement, the European Commission's Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield,[78] was as well declared "invalid" by the CJEU in a judgment handed down on 16 July 2020.[79] As a result of that decision, the EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States. The decision does not relieve participants in the EU-U.S. Privacy Shield of their obligations under the EU-U.S. Privacy Shield Framework with the effect that it may not play a significant role in the design of guidelines for the working of EURHISFIRM at the moment. Standard contracts which could be acknowledged suffer from the same flaws like the Privacy Shield since according to the Foreign Intelligence Act (FISA) of the United States search and seizure of foreign data could be performed without any judicial control.

3.3. Law of the Member States

3.3.1. Foundations

Until 25 May 2018, all EU Member States had implemented the (preceding) Directive 95/46/EC[80] through comprehensive national data protection law, consisting of at least general data protection statutes and in most cases additional sector specific rules.

As of 25 May 2018, the GDPR is *directly applicable* law in the Member States. Directive 95/46/EC explicitly has been repealed and thus is no law any more. As regards EURHISFIRM this binding force of the EU law is obvious for the participants from Member States. The specific case of the UK will be treated in more depth in the following Section 3.4.

As directly applicable EU law the GDPR has precedence over any national law, even constitutional law. In case of inconsistencies between the rules of the GDPR and national law, the principle of *primacy of application* of the law of the EU (*Anwendungsvorrang*) needs to be observed. Even if the principle of precedence is still debated in the legal literature[81] and relativised to some extent by the GFCC,[82] the

[77] Judgment in Case C-362/14, 16/07/2020, *Maximillian Schrems v Data Protection Commissioner* [*Schrems II*], ECLI:EU:C:2015:650.
[78] COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), OJ L 207/1, 1.8.2016; see also COMMISSION IMPLEMENTING DECISION (EU) 2016/1251 of 12 July 2016 regarding data in fisheries, OJ L 2017/113.
[79] Judgment in Case C-311/18 of 16/07/2020, *Facebook Ireland, Maximilian Schrems* v *Data Protection Commissioner,* [*Schrems II*], ECLI:EU:C:2020:559.
[80] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23.11.1995.
[81] See for details *Kruis*, Der Anwendungsvorrang des EU-Rechts in Theorie und Praxis, 2013.
[82] Case law on fundamental rights; for details see *Ludwigs/Sikora,* EWS 2016, 121.

CJEU sternly adheres to it.[83] For all practical purposes it should be understood that in case of doubt EU law *prevails*.

From this it follows that the GDPR leaves no room for additional comprehensive national data protection rules. National data protection rules can no longer be stand-alone comprehensive sets of rules. Any national data protection law therefore only sits alongside the GDPR. The national law can either only be a fragment supplementing the (comprehensive) rules of the GDPR or can repeat them verbatim. Diverging national content in the respective Member States can only be minute. The CJEU has emphasized the uniform application of EU law when it regulates a specific field:

> In that regard, it should be noted that, the need for a uniform application of EU law and the principle of equality require that the wording of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union (judgments of 26 March 2019, SM (Child placed under Algerian kafala), C-129/18, EU:C:2019:248, paragraph 50, and of 11 April 2019, Tarola, C-483/17, EU:C:2019:309, paragraph 36).[84]

(8) Guideline for EURHISFIRM

The statutory rules of the Member States are a source of law, to be observed by EURHISFIRM but with a greatly diminished importance as consequence of the primacy of the comprehensive EU harmonisation by the GDPR, which is directly binding law in all Member States. But a substantial number of outright opening clauses or spaces for interpretation and (legal) circumvention exist. As a result the situation appears quite fragmented despite the original intention to create a widely harmonised legal playing field, demonstrated by the replacement of the Directive through a Regulation.

3.3.2. Space for Legal Rules of the Member States

Margins for autonomous decisions of the Member States thus exist. Since harmonisation of data protection law is according to Article 3 TFEU not an exclusive competence of the Union, national law of the Member States may in principle supplement it. This might be in particular true in the case of international (bilateral) treaties, however subject to the exclusive competence of the Union from Art. 3(2) TFEU and to an exhaustive regulation of a subject matter by Union law. As a general rule, it has to be kept in mind that the GDPR is a *codification* which by its very nature is designed to be comprehensive and exhaustive. Hence, often it has to be decided on a case by case basis where on to what extent competences remain with the Member States. It is clear where an outright opening clause exist. But this is only in some areas the case. Often it is a question of interpretation and – eventually –

[83] CJEU, case 6/64 of 15/7/1964, *Costa/E.N.E.L.*, ECLI:EU:C:1964:66, collection of cases 1964, 1251 (1269 f.); comment by *Frowein,* RIW/AWD 1964, 258, p. 5 et seq. with further references.
[84] CJEU case C-673/17 of 1 October 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV* v *Planet49 GmbH,* ECLI:EU:C:2019:801, margin number 47.

the delineation will be left to court decisions. Contrary to the original intentions of the GDPR, the area thus appears for the persons subjected to the regulations quite fragmented.

As far as opening spaces for national law are left, it has to be kept in mind that the EU-law is "blind" in view of the internal organization and distribution of competences *within* a Member States. It treats them as one unit no matter if they are a centralized state or some kind of a federal system. In contrast to the stylized view in political sciences or parts of the work of economists on federalism, there is *no federalism as such*. A great variety has to be observed at closer scrutiny. In effect, it is not even possible to state universal rules for the group of federal systems within the EU. Even the federal systems in the German speaking world, like Austria and Germany, show differences which make it almost impossible to present overarching rules. As a result, in-depth analysis is mandatory in order to decide which entity is granted which powers and competences by the national law in a field not harmonized by the EU. This holds in specific for Germany where the distribution of competences in the area of the protection of personal data, but not so much for the protection of privacy, is split between the central government and the states. Moreover, it has to be distinguished between the creation of rules, mainly by parliamentary legislation or executive orders, and the application of the (statutory) rules.

As regards the public law entities of a state, in Germany, the states command considerable competences in the field of data protection[85] and have adopted their own data protection laws. This is particularly relevant for research institutes and universities since they are regularly organized as public law entities *of the various states*. For a research institution within the Johann-Wolfgang-Goethe-Universität in Frankfurt, as an example, the "*Hessische Datenschutzgesetz*" would be applicable.[86] Under certain circumstances this would even hold for private law entities under the supervision of those public law entities.[87]

The GDPR has to be considered as a comprehensive and exhaustive regulation of the protection of privacy and personal data. It was intended to be conclusive and not only setting a minimum standard: "In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member

[85] This has to be derived from excluding formulation in Section 1 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*) regulating its area of application:

> *"(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch*
> *1. öffentliche Stellen des Bundes,*
> *2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie*
> *a) Bundesrecht ausführen oder*
> *b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt."*

[86] Section 1(1) Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) vom 3. Mai 2018

[87] This follows from the definition in Section 2(1) HDSIG: *(1) [1]Öffentliche Stellen sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Landes, der Gemeinden und Landkreise oder sonstige deren Aufsicht unterstehende juristische Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. [2]Nimmt eine nicht öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.*

States."[88] Its explicit objective is "to prevent divergences hampering the free movement of personal data within the internal market".[89] Even if a full harmonisation was not envisioned, individual Member States should only have space to impose further specifications on particular topics if and to the extent an opening clause allows them to do so:[90]

> [The] Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.[91]

It follows from this that (diverging) national rules are admissible only if and to the extent they are expressly permitted for a defined subject matter or if they don't fall into the domain of the GDPR. In these cases the Regulation does not "exclude" Member State law and space for (diverging) legal rules of the Member States exist and may have to be observed by EURHISFIRM. This space may be a cause for "some legal uncertainties".[92]

One point that might be relevant for EURHISFIRM is the protection of the privacy of deceased persons.[93] It will be treated more extensively in Sections 6(6.2)(6.2.4) and 0(7.1).

(9) Guideline for EURHISFIRM

In general, the GDPR is exhaustive and conclusive, thus foreclosing national regulation in the field of data protection and privacy save opening clauses.

3.3.3. Overview of National Law on the Protection of Privacy and Personal Data

With the described caveats the statutory rules of the following seven jurisdictions might have to come into consideration:

- Belgium (i)
- France (ii)
- Germany (iii)
- The Netherlands (iv)
- Poland (v)
- Spain (vi)

[88] Recital 10 sentence 1 GDPR.
[89] Recital 10 sentence 1 GDPR
[90] *Rücker,* in: Rücker/Kugler, margin number 9.
[91] Recital 10 sentence 5 et seq.
[92] *Rücker,* in: Rücker/Kugler, margin number 10.
[93] See Recital 27 GDPR.

- The UK (Northern Ireland) (vii)

The following overview on national data protection law is not exhaustive and would have to be verified nationally.[94] In any case it does not include the national legislation implementing the Law Enforcement Directive, which is not relevant for EURHISFIRM.[95]

i. Belgium

General national data protection legislation:

- Law on the protection of individuals with regard to the processing of personal data of 30 July 2018 (the Framework Act);
- Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[96];

National Data Protection Supervisory Authority:

Commission de la Protection de la Vie Privée/Gegevensbeschermingsautoriteit[97]

ii. France

General national data protection legislation:

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[98]

National Data Protection Supervisory Authority:

[94] For details see *Tani* and *van der Hof* (2018), Computer Law & Security Review 34(2), 234-243; available at: http://www.sciencedirect.com/science/article/pii/S0267364917302856 (accessed: 20 January 2021); Roßnagel/ Bile/Friedewald/Geminn/Grigorjew/Karaboga/Nebel (2018), National implementation of the general data protection regulation, available at: http://publica.fraunhofer.de/documents/N-481274.html (accessed: 20 January 2021). Several international law firms provide overviews on data protection regimes worldwide, e.g.: DLA Piper: https://www.dlapiperdataprotection.com; Linklaters: https://www.linklaters.com/en/insights/data-protected/home.

[95] See above section 3.2.

[96] In the Belgian Official Journal (Belgisch Staatsblad), the Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel is available at: http://www.ejustice.just.fgov.be/mopdf/2018/09/05_1.pdf#Page10.

[97] Website: https://www.autoriteprotectiondonnees.be/professionnel; https://www.datenschutzbehorde.be/zivilist.

[98] The "Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés" has been renamed "La loi Informatique et Libertés de 17 juin 2019". It has also been adapted to the new legal situation after the GDPR went into force. A well-made (semi-official) full text of the statute is provided on the website of the French Data Protection Supervisory Authority (CNIL) under: https://www.cnil.fr/fr/la-loi-informatique-et-libertes. Additional French national rules and regulations are provided under: https://www.cnil.fr/fr/cadre-national.

Commission Nationale de l'Informatique et des Libertés[99]

iii. Germany

General national data protection legislation:

Bundesdatenschutzgesetz (BDSG)[100]; Landesdatenschutzgesetze

National Data Protection Supervisory Authorities:

Federal Data Protection Commissioner (*Bundesdatenschutzbeauftrage*)[101], sixteen State Data Protection Commissioners (*Landesdatenschutzbeauftragte*), one for each state.[102]

The Federal Data Protection Commissioner (*Bundesdatenschutzbeauftragte*) is, in principle, not competent regarding public bodies on state level, Section 1(1) no 1.

iv. The Netherlands

General national data protection legislation:

- Dutch GDPR Implementation Act: Uitvoeringswet Algemene Verordening gegevensbescherming (UAVG)[103]
- For the use of data from a Personal Records Database: Personal Records Database Act

National Data Protection Supervisory Authority:

Autoriteit Persoonsgegevens[104]

[99] Website: https://www.cnil.fr.
[100] Bundesdatenschutzgesetz (BDSG), Art. 1 des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU – DSAnpUG-EU, vom 30. Juni 2017, BGBl. I [German Federal Law Gazette, part I], p. 2097.
[101] *Der oder die Bundesbeauftrage für den Datenschutz und die Informationsfreiheit,* Chapter 4 BDSG.
[102] A list with all German data protection authorities is available on the Federal Data Protection Commissioner´s website under: https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html.
[103] In the Dutch Official Law Gazette, the Uitvoeringswet Algemene Verordening gegevensbescherming (UAVG) is available under: https://wetten.overheid.nl/BWBR0040940/2020-01-01/0/. An unofficial English translation of the UAVG is available under: https://www.thedatalawyers.com/post/english-translation-dutch-gdpr-implementation-act.
[104] Website: https://autoriteitpersoonsgegevens.nl/nl.

v. Poland

General national data protection legislation:

Act of May 2018 on the Protection of Personal Data[105]

National Data Protection Supervisory Authority:

Biuro Generalnego Inspektora Ochrony Danych Osobowych (GIODO)[106]

vi. Spain

General national data protection legislation:

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[107]

National Data Protection Supervisory Authority: aepd – Agencia Espanola Proteccion Datos[108]

vii. The UK (Northern Ireland)

General national data protection legislation:

UK Data Protection Act 2018 (DPA 2018)[109]

National Data Protection Supervisory Authority:

UK Data Protection Supervisory Authority (Information Commissioner's Office – ICO)[110]

[105] A link to an English translation of the national data protection act is provided on the website of the Polish Data Protection Supervisory Authority under: https://www.uodo.gov.pl/en/594. The Polish original-language version is also be provided on the GIODO´s website.
[106] Website: https://archiwum.giodo.gov.pl.
[107] A Link to Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales is provided on the website of the Spanish Data Protection Supervisory Authority (aepd) under: https://www.aepd.es/es/informes-y-resoluciones/normativa-y-circulares.
[108] Website: https://www.aepd.es/es. Information on its website is currently provided in Spanish only.
[109] The DPA 2018 is available under: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
[110] Website: https://ico.org.uk.

The DPA 2018 replaced the Data Protection Act 1998, which implemented – until 25 May 2018 – the EU Data Protection Directive 95/46/EC in UK law.[111] More information by the ICO on the DPA 2018 and on Brexit is available on the ICO's website.[112]

3.4. The Special Situation of the EURHISFIRM Participants from the UK

3.4.1. The Transition Period

The UK has withdrawn from the EU by notification of 29 March 2017.[113] Following Article 50 TEU (in conjunction with Article 106a of the Euratom Treaty) the law of the Union (and of Euratom) have ceased to apply to the United Kingdom, though subject to the arrangements of the Withdrawal Agreement.[114] The Withdrawal Agreement entered into force on 1 February 2020, after having been agreed on 17 October 2019, together with the Political Declaration setting the framework of the future EU-UK partnership, Article 185 Withdrawal Agreement.[115] In order to achieve an orderly withdrawal[116] it was consented that during a "transition period (…) Union law, including international agreements, should be applicable to and in the United Kingdom, and, as a general rule, with the same effect as regards the Member States", Article 127(1) subparagraph 1 Withdrawal Agreement. This way a "disruption in the period during which the agreement(s) on the future relationship will be negotiated" was to be avoided.[117] The exceptions to this general rule in Article 127(1), subparagraph 2 are not relevant for EURHISFIRM.

The general rule is subject to special regulations of the Withdrawal Agreement. Such special regulations have been adopted in Title VII of the Agreement headlined "Data and Information Processed or obtained before the end of the transition period, or on the basis of this agreement". As part of this title, Article 71(1) orders as a general rule that "Union law on the protection of personal data law" will remain in force, albeit with a few modifications. The term "Union law on the protection of personal data law" is defined by Article 70 in a quite extensive manner encompassing:

- Regulation (EU)2016/679 (GDPR)[118] – with exception of Chapter VII thereof treating cooperation of institutions, consistency of application, and the European data protection board;
- Directive (EU) 2016/680 (DPD)[119];

[111] It is still available from the UK national law database under https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf.
[112] https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/.
[113] See AGREEMENT on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, Preamble, first Paragraph, OJ L 29/7, 31.1.2020.
[114] Withdrawal Agreement (footnote 113), Preamble, paragraph 4.
[115] Notice concerning the entry into force of the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, L 29/189, 31.1.2020.
[116] Withdrawal Agreement (footnote 113), Preamble, paragraph 5.
[117] *Ibid*. paragraph 8.
[118] For reference see footnote 56.
[119] For reference see footnote 62.

- Directive 2002/58/EC[120];
- any other provisions of Union law governing the protection of personal data.

Hence its material scope is comprehensive.

Deviating substantive rules are mainly set up for data processing outside the EU and the UK. This affects the Shield Agreement between the EU and the USA, which has meanwhile anyhow been declared invalid by the CJEU in its *Schrems II* judgment.[121] The other rules refer to information security, confidentiality and organisational questions.

(10) Guideline for EURHISFIRM

In principle, during the transition period the same legal rules continue to be in force which govern the set-up and working of EURHISFIRM.

According to Article 2(e) in conjunction with Article 126 of the Withdrawal Agreement, the transition period was to end on 31 December 2020 and a new agreement on the future relationship (or an extension of the transition period) would have to be concluded in order to avoid an "unorderly" break-up. The framework for this agreement had already been set out in the political declaration of European Council summit on 17 October 2019 together with the Withdrawal Agreement. Nevertheless, until the very end of the period it looked as if the goal would be entirely out of reach.

3.4.2. The Relationship after the Transition Period

It took long and often painful negotiations to reach a consensus on the terms of the *withdrawal* of the UK from the EU but finally the Withdrawal Agreement[122] was signed and ratified. An agreement on the *future relationship* between the European Union and the United Kingdom, to be thoroughly distinguished from the Withdrawal Agreement, seemed to be even more difficult to reach. On 30 December 2020, however, almost at the last minute of the transition period, an "EU-UK trade and cooperation agreement" (TCA) was signed[123] unfolding on more than 1200 pages the rules governing the (future) relationship.

Already in the Preamble of the Trade and Cooperation Agreement[124] the rules on "personal data protection" are mentioned[125] but the Parties to the Agreement reaffirm the right to regulate within

[120] For reference see footnote 64.
[121] For reference see footnote 79.
[122] See footnote 113.
[123] Press release of the Council of the EU: https://www.consilium.europa.eu/en/press/pressreleases/2020/12/30/press-release-signature-of-the-eu-uk-agreement-30-december-2020/pdf.
[124] TRADE AND COOPERATION AGREEMENT BETWEEN THE EUROPEAN UNION AND THE EUROPEAN ATOMIC ENERGY COMMUNITY, OF THE ONE PART, AND THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, OF THE OTHER PART, OJ L 444/14, 31.12.2020.
[125] Paragraph 11.

their territories "privacy and data protection".[126] The protection of personal data and privacy is confirmed as a fundamental right of all individuals.[127] The topic data protection is taken up in Article COMPROV.10 where the Parties confirm in general terms "their commitment to ensuring a high level of personal data protection and privacy".[128] Specific rules are approved for the transfer of personal data.[129]

(11) Guideline for EURHISFIRM

As of 1 January 2021 the agreement on "trade and cooperation" between the United Kingdom and the EU serves as the relevant legal regime, especially in view of the EURHISFIRM participant from the UK, albeit so far on a provisional basis.

3.4.3. Digression: Assessment of the Legal Situation in the Time of Incertitude

When assessing the (future) legal situation always *two different perspectives* have to be taken into account: the EU law and the national law of the UK. Both perspectives have to be applied when evaluating the different developments, especially if the transition period ended without a bilateral agreement between the EU and the UK.

i. No agreement is reached

In the case of the transition period ending without a bilateral agreement between the EU and the UK, the different perspectives outlined above, two crucial questions would need to be assessed and answered separately:

- What are the then applicable national rules in the UK to transfer personal data from the UK to another country?
- What are the then applicable rules to transfer personal data from the EU to the UK?

From the EU's perspective the general rules of the GDPR would remain the same. The EU law would treat the UK as "third country" and all the restrictive provisions on data transfer and data processing outside the EU laid down in Chapter V of the GDPR would apply.

[126] Part Two, Title II: Services and Investment, Chapter 1: General Provisions, Article SERVIN.1.1: Objective and scope [OJ page 130]; Chapter 2: Data flows and personal data protection, Article DIGIT.7(2) [OJ page 132].
[127] Chapter 2: Data flows and personal data protection, Article DIGIT.7(1): Protection of personal data and privacy [OJ page 132].
[128] Part Six: Dispute Settlement and Horizontal Provisions, Title II: Basis for Cooperation, Article COMPRO.10: Personal data protection, paragraph 2 [OJ page 420].
[129] Paragraph 4: Where this Agreement or any supplementing agreement provide for the transfer of personal data, such transfer shall take place in accordance with the transferring Party's rules on international transfers of personal data. For greater certainty, this paragraph is without prejudice to the application of any specific provisions in this Agreement relating to the transfer of personal data, in particular Article DIGIT.7 [Protection of personal data and privacy] and Article LAWGEN.4 [Protection of personal data], and to Title I of Part Six [Dispute Settlement]. Where needed, each Party will make best efforts, while respecting its rules on international transfers of personal data, to establish safeguards necessary for the transfer of personal data, taking into account any recommendations of the Partnership Council under point (h) of Article INST.1(4) [Partnership Council].

What the UK law will eventually command is open. By act of parliament, the UK might transpose the present provisions of EU law into national law and later declare them binding legal rules in the UK. This could be achieved by extending the UK's European Union (Withdrawal) Act 2018 beyond 31 December 2020. Then the GDPR will form part of UK law. The details hinge on the specific rules of the constitutional law in Great Britain and Northern Ireland. In specific, the peculiarities of the relationship between these two parts of the UK will be relevant for EURHISFIRM since one participating institution resides in Northern Ireland.

The UK might, on the other hand, completely abstain from any legislative action. Then (only) the present rules of the national law will have to be observed. The UK Data Protection Act 2018 (DPA 2018)[130] will remain in force but in substance it has to be considered a fragment without the rules set by the GDPR. An interesting legal question would be whether the Data Protection Act 1998[131] which was in force before the GDPR was enacted would automatically be resuscitated in case of a total lack of legislative action. In Germany, the answer would depend on the type of derogation. Here, if a statute derogating a norm is void or is repealed the former norm would revive.[132]

In theory, the UK is also free to design a completely new set of legal rules on the protection of privacy and personal data. In view of the problems that would have to be coped with in a "no agreement" situation, this alternative can be treated as highly improbable.

ii. An agreement is reached

In this case, the agreement might either extend the present legal rules relevant for EURHISFIRM into the future or abstain from regulating this sector. The first alternative would have the result that no significant change in the legal situation relevant for EURHISFIRM would take place; both from the EU and the UK legal perspective. Chapter V of the GDPR would not be applicable. The second alternative would, in principle, lead to a similar situation as described before; again from both perspectives.

Obviously, a mixed bouquet of different other solutions is also possible.

iii. Article 8 Withdrawal Agreement

There is, however, a caveat which would become relevant in both alternatives: The Withdrawal Agreement expressly provides in Article 8 that "at the end of the transition period the United Kingdom shall cease to be entitled to access any network, any information system and any database established on the basis of Union law." This clause contains, however, only a general rule and is subject to differing provisions in the Agreement. However, if there exists none, it remains in force. For the operation of EURHISFIRM this alternative has to be kept in mind.

[130] For reference see footnote 109.
[131] For reference see footnote 111.
[132] See BVerwG [Federal Administrative Court], NVwZ 1991, 673 (674); *Konzelmann,* 1997, chapter 3, section 1, first paragraph; see in general *Schneider,* Gesetzgebung, 1991, at margin number 556.

3.4.4. Conclusion

From the perspective of the EU law the "Union law on the protection of personal data law" may in principle stay in force by an act of legislation of the UK. The language of the Trade and Cooperation Agreement is so general that – in a first assessment – nothing bars its continuation. For a new transition period of four months, the UK will not be assessed as an "unsafe" third country, however, under the pre-requisit that it will retain its national data protection law based on the GDPR. Some voices take, however, the view that EU law does not allow such a separate regulation as regards the UK. The counter argument points to the legality of treaties under the law of nations between the EU and a third country.[133]

Now to turn to the national law of the UK. The UK parliament adopted on 31 December 2020 a European Union (Future Relationship) Act 2020 taking effect from 1 January 2021 (on a provisional basis). As a first assessment, it can be said that most of the rules of the Data Protection Act 2018 are retained save the rules on criminal records and the duty to notify (Part 1, sections 1-3). This needs, however, a more in-depth analysis of this act in conjunction with the Data Protection Act 2018, which in principle adopts the EU law.

Section 7A of EUWA provides for the UK-EU Withdrawal Agreement, including the Northern Ireland Protocol, to have direct effect in the UK legal system where the agreement requires this. Section 29 of the European Union (Future Relationship) Act 2020[134] similarly makes a general modification to all existing domestic law, so far as necessary to comply with the UK-EU Trade and Cooperation Agreement.[135]

Thus, until the end of April 2021 data traffic may freely flow between the EU and the UK. This deadline may be extended by another period of two months.[136] At the end of June, as latest, the Commission has to approve the national law as adequate to continue rules about free flow of data.[137]

(12) Guideline for EURHISFIRM

The legal situation for EURHISFIRM and the participant from the UK after the end of the transition period is governed by the agreement of December 2020 and the European Union (Future Relationship) Act 2020 of the UK. An ongoing incorporation of the GDPR rules into UK law has been provided for. In any case Article 8 of the Withdrawal Agreement has to be taken into account. An adequacy decision of the Commission is necessary, the latest by 30 June 2021.

4. Confinement to Data Relating to Natural Persons

In contrast to intellectual property rights[138] not all the information expressed in a database or the database as such in which that information is contained is a suitable subject for legal protection by the

[133] *Heidrich,* c't 2021, page 26.
[134] See for the Bill: https://publications.parliament.uk/pa/bills/cbill/58-01/0236/20236.pdf.
[135] https://www.pinsentmasons.com/out-law/guides/retained-eu-law-uk-after-brexit
[136] *Heidrich,* c't 2021, page 26.
[137] *Ibid.*
[138] Report WP 3.1.

statutory rules on privacy or personal data. In so far, a substantial difference from Work Package 3.1 has to be recognised whereas – once a suitable subject matter of protection has been identified – the regulation of the different phases of treatment, the extraction, the copying of such source material and its further processing are regulated in a comparable way.

In view of the data to be collected and processed in the context of EURHISFIRM it is of *utmost importance* to note that the protection of privacy or personal data is restricted to information related to *natural persons*. Legal persons, like corporations or associations, do not enjoy this protection.[139] A legal entity cannot have privacy in the legal sense of the word, even if secrecy and confidentiality exist in businesses and administrations. If it is made available to the public, the legal protection of data and of the underlying (general) personality right is only affected if, and only if information on an identifiable natural person is concerned. The data used by a company might be crucial for its existence but it is not protected by the data protection statutes. This reduces the relevance of the following considerations for the practical work of EURHISFIRM greatly.

This confinement to data concerning natural persons is expressly contained in Articles 1(1)(2) and 4(1) GDPR. From the latter clause can also be gathered that the term "personal data" means only information relating to a natural person. It is labelled there as "data subject". With almost identical wording this limitation is also emphasised in Article 1(1) IDPR and Article 1(1) DPD. Apart from this far-reaching limitation, a broad interpretation of "privacy" and "private life" has to be followed.[140]

The protection of privacy might, however, go further if another, specialized norm orders this. An example is Article 5(3) ePrivacy Directive, it regulates information "irrespective of whether the information stored … contains personal data or not." The provision refers to "the storing of information" and "the gaining of access to information already stored", without characterising that information or specifying that it must be personal data."[141] It aims "to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data".[142]

The new ePrivacy regulation, which is still in the legislative process[143] will repeal the existing ePrivacy directive. As *lex specialis* to the general data protection regulation (GDPR), it will particularise and

[139] Recital 14 GDPR: "This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person."
Recital 6 IDPR: "This Regulation should not apply to the processing of personal data of deceased persons. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person."
[140] See European Court of Human Rights, case *Amann v Switzerland,* 16/2/2000, para 65.
[141] CJEU case C-673/17 of 1 October 2019, *Bundesverband der Verbraucherzentralen und Ver-braucherverbände — Verbraucherzentrale Bundesverband eV* v *Planet49 GmbH*, E-CLI:EU:C:2019:801, margin number 68.
[142] Ibid, at margin number 69.
[143] See proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) of 10.1.2017, COM(2017) 10 final. 2017/0003 (COD)

complement the GDPR. For example, in contrast to the GDPR, many ePrivacy provisions will apply to both natural and legal persons.[144]

As already mentioned in the report on Work Package 3.1, for the creation of any database, the gathering and eventual presentation of data is a key component. In order to gather data an extraction from various sources is necessary. Different media can be used as sources for firm data, e.g. public (commercial) registers, stock market lists, corporate yearbooks, newspapers, secondary literature or other databases whether in print or electronic form. In some cases, the inclusion of the original sources or images thereof in the database has to be considered.

However, all these sources contain little or no information related to natural persons. The firm data EURHISFIRM is interested in are mainly related to legal entities and not to natural persons. Almost never do they contain sensitive data which enjoy special protection under the data protection laws. They mainly contain financial information or information about the organisation of the entity, i.e. specifically about the legal status of the entity but in addition sometimes about (natural) persons instituted as their representatives or having power to act on behalf of them. Here the laws protecting privacy and personal data might be relevant.

(13) Guideline for EURHISFIRM

As data on the financial situation of firms or prices in a stock exchange usually contain little or no information related to natural persons the significance of legal rules protecting them is very limited for EURHISFIRM. This holds true especially for stock exchange reports. However, as far as natural persons behind them or acting on behalf of them are identifiable they might be relevant.

5. Primary Law of the European Union

5.1. Charter of Fundamental Rights of the EU (CFR)

5.1.1. Article 7 CFR

The protection of privacy is one of the most important objectives of Article 7 CFR. It stipulates the respect for private and family life by laying down the right of every person to respect for his or her private and family life, home and communications. Thus, it combines four aspects of the private sphere, which are spread over several clauses in many codifications, in one provision.[145]

The majority of the rights are by their nature limited to natural persons. The bearer of the right to protect communication can be a legal person. Questionable is the extension to some traits of private life and of the "home".[146] Irrespective of this question the provision has to be interpreted in a wide manner. The object of its protection, "private life", "comprises the right to establish and develop

[144] Press release of 10 February 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/.
[145] See *Wolff,* in: Pechstein/Nowak/Häde, 2017, Article 7 CFR margin number 1.
[146] In favour of a wider interpretation *Wolff,* in: Pechstein/Nowak/Häde, 2017, Article 7 CFR, margin number 12.

relationships with other human beings: furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life".[147]

When the provision was being framed, the term "protection" could not garner the necessary approval and the term "respect" was inserted. From this it can be gathered that the wording has been chosen knowingly and purposely. As a result the wording has to be interpreted as being weaker than "protect".[148] In the first place, it is directed to all sovereign powers.[149] Whether it can be extended to other entities is questionable but such has been the most recent case law of the CJEU in its *Schrems II* judgment of 16 July 2020 as regards the practice of Facebook.[150]

Its relevance for EURHISFIRM would be open. There is, however, no need to expound this question in further depth since it is hardly imaginable that the working of EURHISFIRM would ignore the due respect.

5.1.2. Article 8 CFR

Article 8(1) states the protection of personal data: "Everyone has the right to the protection of personal data concerning him or her." It is *lex specialis* as regards Article 7 of the Charter.[151] In effect, Article 8 CFR has to be considered as the only source of the right of informational self-determination in the primary law of the EU.[152] It serves now as the material basis for the much more elaborated rules of the secondary law. Both Articles are, however, in principle only applicable for living persons.[153] For practical purposes, the regulation of the secondary law have to be considered in the first place.

Article 8(2) of the Charter states the crucial prerequisites for the processing of personal data: "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

The general retention of personal data has been judged as unlawful by the CJEU even if only meta-data were to be retained.[154] In *Schrems I* the Court ruled that mass surveillance measures would compromise the essence of the fundamental right.[155] In *Schrems II* it reaffirmed the importance of the fundamental rights enshrined in Articles 7 and 8 CFR[156] and judged that the communication of personal data to a third party "constitutes the processing of personal data in the meaning of the fundamental rights".[157]

[147] See in different context: European Court of Human Rights, case *Amann v Switzerland,* 16/2/2000, para 65.
[148] *Wolff,* in: Pechstein/Nowak/Häde, 2017, Article 7 CFR, margin number 13.
[149] *Wolff,* in: Pechstein/Nowak/Häde, 2017, Article 7 CFR, margin number 30.
[150] C-311/18 *Schrems II*, ruling 1.
[151] *Wolff,* in: Pechstein/Nowak/Häde, 2017, Article 7 CFR margin number 3, 62.
[152] *Wolff,* in: Pechstein/Nowak/Häde, 2017, Article 7 CFR margin number 3.
[153] *Ernst,* in: Paal/Pauly, Article 1 GDPR margin number 12.
[154] CJEU Case C-203/15 *Tele2 v Sverige,* at paras 99, 155-57; partially critical *Brkan,* German Law Journal (2019), 864, 871-874.
[155] Case C-362/14 *Schrems I,* at margin numbers 1, 84-87.
[156] Case C-311/18 *Schrems II,* at margin number 169.
[157] Ibid. at para 171.

Although this provision is directed primarily at the actions of sovereign entities, including its subsidiaries and subsections,[158] the GDPR nevertheless to a large extent also regulates the activities of private persons. The Charter does not bind explicitly private persons but limited obligations are derived from it by the literature.[159] EURHISFIRM and its participants act, however, not as private persons but as functionaries of state entities fulfilling public duties. Hence it should be taken as given that the clause is applicable to EURHISFIRM.

The CJEU, however, referring to its older case law,[160] emphasised that the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society. In general, it can be assumed that the detailed rules of the GDPR fulfil the requirements of Article 8 CFR and that – for all practical purposes – EURHISFIRM does not breach the rules of the Charter if it complies with the specific regulations of the GDPR.

(14) Guideline for EURHISFIRM

When processing personal data in the Union the following fundamental rules, reiterated and elaborated by the secondary law of the Union, are crucial:

- Specification of the purpose(s),
- Consent of the person concerned or legitimate basis laid down by (statutory) law,
- Right to access to the data,
- Right to rectification.

The practical relevance of the Charter for the working of EURHISFIRM is limited.

5.2. Article 16 of the Treaty on the Functioning of the European Union

The first paragraph of Article 16 TFEU restates the fundamental right to the protection of privacy and personal data also contained in Article 8(1) CFR. Initially, it was developed in the case law of the GFCC[161] and the CJEU.[162] It is now constant judicature[163] and concretised by the secondary law of the

[158] *Pache,* in: Pechstein/Nowak/Häde, 2017, Article 51 CFR margin number 16.
[159] *Pache,* in: Pechstein/Nowak/Häde, 2017, Article 51 CFR margin number 38
[160] CJEU Case C-311/18 *Schrems II,* at para 172: "see, to that effect, judgments of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48 and the case-law cited, and of 17 October 2013, *Schwarz*, C-291/12, EU:C:2013:670, paragraph 33 and the case-law cited; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 136".
[161] BVerfGE 65, 1 (informational self-determination – judgment on census); 100, 313; 115, 166 (online search); 120, 274 (protection of information technology).
[162] Joined cases C-465/00, C-138/01, and C-139/01, *Court of Audit – Austrian Broadcasting System*, ECR 2003 I-4989 margin number 68; C-101/01, *Lindqvist*, ECR 2003 margin number 87.
[163] CJEU: C-275/06, *Promusicae*, ECR 2008 I-271 margin number 63; C-524/06, *Heinz Huber*, ECR 2008 I-9705; C-301/06 of 8/4/2014, *Ireland v Parliament and Council*, ECR 2009, I-593 margin number 47; C-362/14 of 6/10/2015, *Maximillian Schrems v Data Protection Commissioner* [*Schrems I*]; C-203/15 of 21/12/2016, *Tele2 Sverige* (meta-data retention); C-311/18 of 16/07/2020, *Facebook Ireland v Schrems,* ECLI:EU:C:2020:559 [*Schrems II*]; GFCC: e.g. BVerfGE 120, 351, 128, 1; 133, 277; 146, 1.

Union. For all practical purposes, it can be assumed that these concretisations fully comply with the obligations from this fundamental right. However, in case of an interpretation in doubt, the clause may still play an important role in the application of the law.

The second paragraph of Article 16 TFEU creates a sound basis for the competence of the EU which was not beyond any doubts before. This was also the reason why the predecessor of the GDPR was only a directive. Again, for all practical purposes, in specific for the creation and working of EURHISFIRM, it can be assumed that the GDPR fulfills the obligations from this clause but also stays within the limits of the granted competence.

6. The General Data Protection Regulation

A comprehensive reform of the data protection rules in the EU took place in 2016. The new General Data Protection Regulation (GDPR) was created and it entered into force on 25 May 2016.[164] Pursuant to Article 99(2) GDPR, the commencement of its application was postponed to 25 May 2018. As already mentioned, of the EU secondary law only the GDPR is relevant in substance for EURHISFIRM. The focus of the following reflections is on this Regulation.

6.1. Objectives

The Regulation is designed to protect "fundamental rights and freedoms of natural persons" in general but "in particular their right to the protection of personal data" (Article 1(2) GDPR). The free movement of data within the Union, however, "shall be neither restricted nor prohibited" by the rules set up by the Regulation (Article 1(3) GDPR).

The rules of the GDPR are intended to give citizens control over their personal data (back). It has to be kept in mind that the protection of natural persons in relation to the processing of personal data is a fundamental right. Articles 8(1) CFR and 16(1) TFEU provide that everyone has the right to the protection of personal data concerning him or her. This right is also guaranteed under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.[165]

6.2. Confinement to Personal Data

The object of the protection by the Regulation can only be "personal data".

6.2.1. The Information Covered

From the definition of personal data in Article 4(1) it follows that "personal data" has to be understood in a *very wide sense*. It covers any type of information.[166] In particular, the relationship between a natural person and an object can be included. The simple fact of ownership is personal data if it relates to a natural person. An entry in a public register suffices. This can be specifically relevant in view of real estate and its recording in public registers or a registration as a stock corporation.

[164] For reference see footnote 56.
[165] See Section 3(3.1).
[166] CJEU case C-434/16 *Nowak,* at para 4; *Rücker,* in: Rücker/Kugler, 2018, margin number 72; *Klar/Kühling*, in: Kühling/Buchner, 2020, Article 4 No 1 GDPR margin number 8.

6.2.2. The Requirement of Natural Persons as Data Subjects

The general confinement of the legal provisions protecting data and privacy to information on natural persons[167] is intensified and specified by the GDPR: Not only does Article 1(2) GDPR expressly confine the Regulation to the protection of natural persons but also Article 1(1) GDPR states that the rules laid down in the Regulation (*only*) relate to the protection of *natural persons.* This fundamental restriction is reiterated in Article 4(1) GDPR legally defining them as "data subjects". Moreover, the clause establishes a link to the term "personal data". For the purpose of the Regulation "personal data" is defined as "any information relating to an identified or identifiable natural person". This implies that the information must relate to a specific natural person and not to a mere category. Consequently the *objects* of the protection are only "personal data" (Article 2(1) GDPR).

6.2.3. Personal Data as Protected Information

a) Link to an Identified or Identifiable Natural Person

The identification can take place by using the name of the natural person. In the case of a very common name, e.g. Smith, Müller, additional information, like time and/or place of birth, might be necessary. The identification can, however, also take place indirectly. It suffices if it is "identifiable". In the language of the Regulation an "identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4(1) GDPR). Physical attributes or character traits of a person can also be used. Opinions, wishes, value judgments might likewise serve as facts about the person's financial situation. All links of a person to third parties or its environment may render it identifiable.[168]

Absolutely anonymised data are no personal data since a link to identified or identifiable person does not exist.[169] The GDPR does not use the distinction between absolute, formal and *de-facto* anonymisation. Since Recital 26 GDPR builds on "objective factors" as obstacles for an identification, in effect a *de-facto* anonymisation should suffice.[170]

---

[167] Treated above in Part 4.

[168] See *Klabunde*, in: Ehmann/Selmayr, Article 4 margin number 7 et seq.; *Klar/Kühling*, in: Kühling/Buchner, 2020, Article 4 Nr. 1 GDPR margin number 19, pointing to the possibilities of a re-identification by big-data analysis (at no 22); *Rücker,* in: Rücker/Kugler, 2018 margin numbers 84 et seq.

[169] This can also be derived from Recital 26 sentence 4: "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

[170] Recital 26 sentence 3: "To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments." For more details see *Watteler/Ebel,* Forschungsdatenmanagement, 2019, pages 66-68.

Already in 2007, the Article 29 Data Protection Working Party (Art. 29 WP)[171] published an in-depth elaboration of the term "personal data".[172] This work is of specific interest since the Art. 29 WP was an advisory body made up of a representative from the data protection authority of each Member State. Thus it might be considered as a "semi-official" interpretation of the law. With the entering into force of GDPR, the "Party" has been replaced by the European Data Protection Board (EDPB).[173]

Anonymised data are no personal data as far as objective factors prohibit the identification of a natural person.[174] In this case since a link to identified or identifiable person does not exist.[175] The GDPR does not use the distinction between

The European Court of Justice has ruled that the term personal data "undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies".[176] In another case it concluded that the IP address of a natural person allows the identification of that person and has to be judged as personal data.[177]

(15) Guideline for EURHISFIRM

EURHISFIRM has to assume that the GDPR uses the term "personal data" in a very wide sense covering any information relating to an identified or identifiable natural person. The name of a person in conjunction with his or her telephone number or information about his or her working conditions or hobbies suffices.

From this follows that information relating to *legal persons* or other such entities is not covered by the Regulation.[178] In exceptional cases, however, data relating to legal persons are covered; provided they allow information to be derived about a natural person standing "behind" the legal entity. This is e.g. the case when a corporation is owned by only one natural person. Then information on the financial situation of the corporation might be "personal data".[179] This can be even more the case in regard to

[171] Its full name is "The Working Party on the Protection of Individuals with regard to the Processing of Personal Data".
[172] Opinion 4/2007 of 20.06.2007 on the concept of personal data (01248/07/EN, WP 136), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, with details about "identifiable" on pages 12 et seq.
[173] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492. The *Board* can be found under the following address: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492.
[174] Recital 26 GDPR.
[175] This can also be derived from Recital 26 sentence 4 GDPR: "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."
[176] C-101/2001 of 6/11/2003, *Lindqvist,* at margin number 24.
[177] C-582/14 of 19/10/2016, *Patrick Breyer v Bundesrepublik Deutschland,* at margin number 47 et seq.
[178] Recital 14 GDPR: "The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person."
[179] WP 136, 24.

a one-person company or a partnership. In rare cases a tightly knit financial, personal, or economic interconnection between the legal person and a natural person might also suffice.

For the purpose of EURHISFIRM it will be important that information relating to a stock corporation as such does not have to be considered as personal data and is not affected by the rules of the GDPR.

(16) Guideline for EURHISFIRM

The GDPR does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of that person. Information collected from stock exchanges will hence be "safe" from legal rules protecting personal data unless they render information about a natural person owning it.

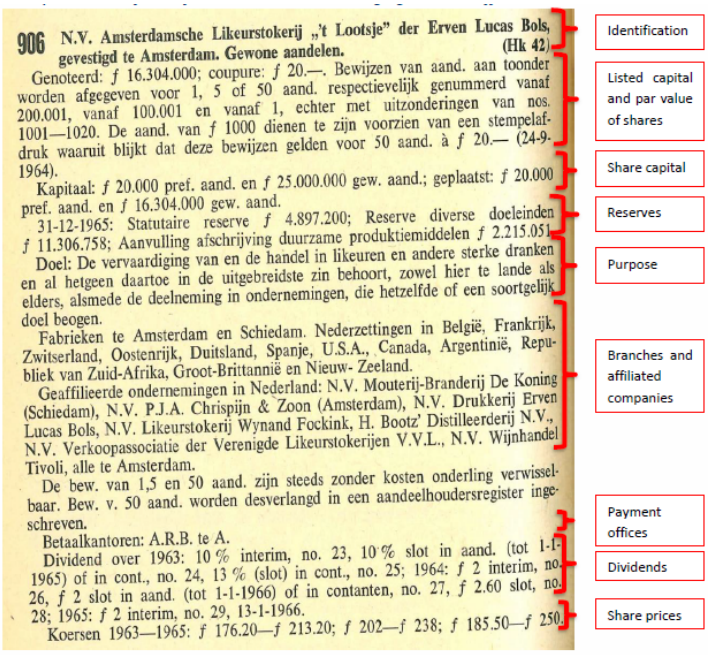
b) Application

The "Report on the Inventory of Data and Sources", EURHISFIRM – D4.2, has presented some examples from yearbooks[180] already assessed by Report 3.1 (as regards the protection of intellectual property):

[180] Pages 117-132.

Example a

Figure 1: Dutch Yearbook, Gids bij de Prijscourant van de Vereeninging voor den Effectenhandel[181]



906 N.V. Amsterdamsche Likeurstokerij „'t Lootsje" der Erven Lucas Bols, gevestigd te Amsterdam. Gewone aandelen. (Hk 42)

Genoteerd: ƒ 16.304.000; coupure: ƒ 20.—. Bewijzen van aand. aan toonder worden afgegeven voor 1, 5 of 50 aand. respectievelijk genummerd vanaf 200.001, vanaf 100.001 en vanaf 1, echter met uitzonderingen van nos. 1001—1020. De aand. van ƒ 1000 dienen te zijn voorzien van een stempelafdruk waaruit blijkt dat deze bewijzen gelden voor 50 aand. à ƒ 20.— (24-9-1964).

Kapitaal: ƒ 20.000 pref. aand. en ƒ 25.000.000 gew. aand.; geplaatst: ƒ 20.000 pref. aand. en ƒ 16.304.000 gew. aand.

31-12-1965: Statutaire reserve ƒ 4.897.200; Reserve diverse doeleinden ƒ 11.306.758; Aanvulling afschrijving duurzame produktiemiddelen ƒ 2.215.051.

Doel: De vervaardiging van en de handel in likeuren en andere sterke dranken en al hetgeen daartoe in de uitgebreidste zin behoort, zowel hier te lande als elders, alsmede de deelneming in ondernemingen, die hetzelfde of een soortgelijk doel beogen.

Fabrieken te Amsterdam en Schiedam. Nederzettingen in België, Frankrijk, Zwitserland, Oostenrijk, Duitsland, Spanje, U.S.A., Canada, Argentinië, Republiek van Zuid-Afrika, Groot-Brittannië en Nieuw- Zeeland.

Geaffilieerde ondernemingen in Nederland: N.V. Mouterij-Branderij De Koning (Schiedam), N.V. P.J.A. Chrispijn & Zoon (Amsterdam), N.V. Drukkerij Erven Lucas Bols, N.V. Likeurstokerij Wynand Fockink, H. Bootz' Distilleerderij N.V., N.V. Verkoopassociatie der Verenigde Likeurstokerijen V.V.L., N.V. Wijnhandel Tivoli, alle te Amsterdam.

De bew. van 1,5 en 50 aand. zijn steeds zonder kosten onderling verwisselbaar. Bew. v. 50 aand. worden desverlangd in een aandeelhoudersregister ingeschreven.

Betaalkantoren: A.R.B. te A.

Dividend over 1963: 10 % interim, no. 23, 10 % slot in aand. (tot 1-1-1965) of in cont., no. 24, 13 % (slot) in cont., no. 25; 1964: ƒ 2 interim, no. 26, ƒ 2 slot in aand. (tot 1-1-1966) of in contanten, no. 27, ƒ 2.60 slot, no. 28; 1965: ƒ 2 interim, no. 29, 13-1-1966.

Koersen 1963—1965: ƒ 176.20—ƒ 213.20; ƒ 202—ƒ 238; ƒ 185.50—ƒ 250.

Identification

Listed capital and par value of shares

Share capital

Reserves

Purpose

Branches and affiliated companies

Payment offices

Dividends

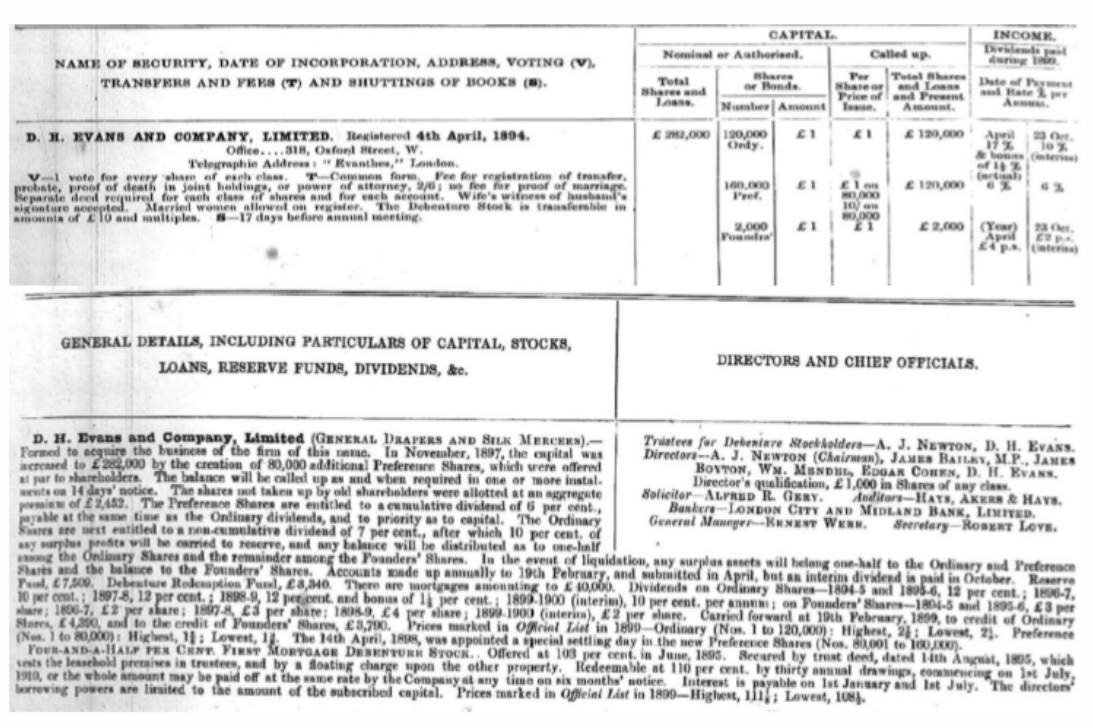
Share prices

An examination in view of the protection of privacy and personal data shows that almost no information relating to an individual natural person is revealed. The identification of the company as "Erven Lucas Bols" might under certain circumstances allow a reader to identify a natural person. The affiliates are mainly organised as N.V., i.e. as an "anonymous" legal subject. Information on the natural persons behind such a legal person are traceable only under extraordinary circumstances or even totally impossible to find.

[181] 1966, page 128.

Example b

Figure 2: British Yearbook, Stock Exchange Official Intelligence[182]



NAME OF SECURITY, DATE OF INCORPORATION, ADDRESS, VOTING (V), TRANSFERS AND FEES (T) AND SHUTTINGS OF BOOKS (S).	CAPITAL. Nominal or Authorised. Total Shares and Loans.	Shares or Bonds. Number	Amount	Called up. Per Share or Price of Issue.	Total Shares and Loans and Present Amount.	INCOME. Dividends paid during 1899. Date of Payment and Rate % per Annum.	
D. H. EVANS AND COMPANY, LIMITED. Registered 4th April, 1894. Office.... 318, Oxford Street, W. Telegraphic Address: "Evanthes," London. V—1 vote for every share of each class. T—Common form. Fee for registration of transfer, probate, proof of death in joint holdings, or power of attorney, 2/6; no fee for proof of marriage. Separate deed required for each class of shares and for each account. Wife's witness of husband's signature accepted. Married women allowed on register. The Debenture Stock is transferable in amounts of £10 and multiples. S—17 days before annual meeting.	£282,000	120,000 Ordy.	£1	£1	£120,000	April 17 % & bonus of 1½ % (actual)	23 Oct. 10 % (interim)
		160,000 Pref.	£1	£1 on 80,000 10/ on 80,000	£120,000	6 %	6 %
		2,000 Founders'	£1	£1	£2,000	(Year) April £4 p.s.	23 Oct. £2 p.s. (interim)

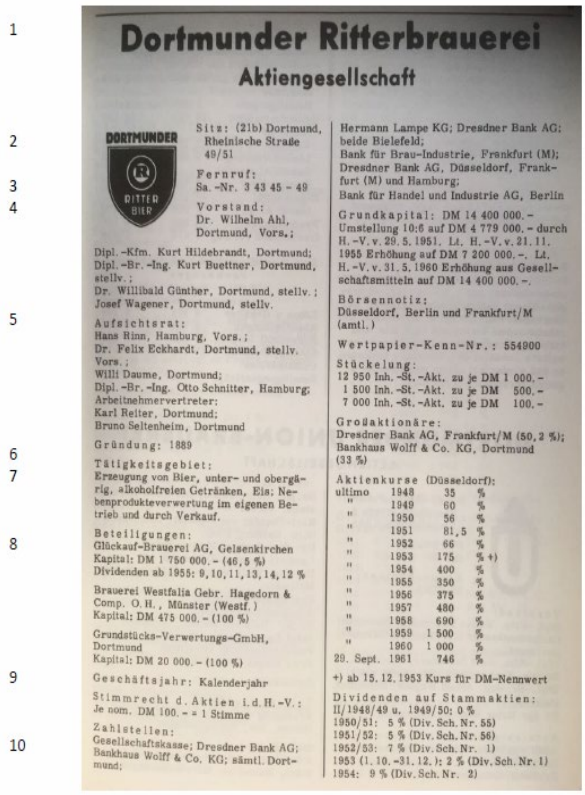
GENERAL DETAILS, INCLUDING PARTICULARS OF CAPITAL, STOCKS, LOANS, RESERVE FUNDS, DIVIDENDS, &c.	DIRECTORS AND CHIEF OFFICIALS.
D. H. Evans and Company, Limited (General Drapers and Silk Mercers).—Formed to acquire the business of the firm of this name. In November, 1897, the capital was increased to £282,000 by the creation of 80,000 additional Preference Shares, which were offered at par to shareholders. The balance will be called up as and when required in one or more instalments on 14 days' notice. The shares not taken up by old shareholders were allotted at an aggregate premium of £2,452. The Preference Shares are entitled to a cumulative dividend of 6 per cent., payable at the same time as the Ordinary dividends, and to priority as to capital. The Ordinary Shares are next entitled to a non-cumulative dividend of 7 per cent., after which 10 per cent. of any surplus profits will be carried to reserve, and any balance will be distributed as to one-half among the Ordinary Shares and the remainder among the Founders' Shares. In the event of liquidation, any surplus assets will belong one-half to the Ordinary and Preference Shares and the balance to the Founders' Shares. Accounts made up annually to 19th February, and submitted in April, but an interim dividend is paid in October. Reserve Fund, £7,500. Debenture Redemption Fund, £3,340. There are mortgages amounting to £40,000. Dividends on Ordinary Shares—1894-5 and 1895-6, 12 per cent.; 1896-7, 10 per cent.; 1897-8, 12 per cent.; 1898-9, 12 per cent. and bonus of 1½ per cent.; 1899-1900 (interim), 10 per cent. per annum; on Founders' Shares—1894-5 and 1895-6, £3 per share; 1896-7, £2 per share; 1897-8, £3 per share; 1898-9, £4 per share; 1899-1900 (interim), £2 per share. Carried forward at 19th February, 1899, to credit of Ordinary Shares, £4,260, and to the credit of Founders' Shares, £3,700. Prices marked in *Official List* in 1899—Ordinary (Nos. 1 to 120,000): Highest, 2½; Lowest, 2⅛. Preference (Nos. 1 to 80,000): Highest, 1⅞; Lowest, 1⅝. The 14th April, 1898, was appointed a special settling day in the new Preference Shares (Nos. 80,001 to 160,000). Four-and-a-Half per Cent. First Mortgage Debenture Stock.—Offered at 103 per cent. in June, 1895. Secured by trust deed, dated 14th August, 1895, which vests the leasehold premises in trustees, and by a floating charge upon the other property. Redeemable at 110 per cent. by thirty annual drawings, commencing on 1st July, 1910, or the whole amount may be paid off at the same rate by the Company at any time on six months' notice. Interest is payable on 1st January and 1st July. The directors' borrowing powers are limited to the amount of the subscribed capital. Prices marked in *Official List* in 1899—Highest, 111½; Lowest, 108½.	*Trustees for Debenture Stockholders*—A. J. Newton, D. H. Evans. *Directors*—A. J. Newton (*Chairman*), James Bailey, M.P., James Boyton, Wm. Mendel, Edgar Cohen, D. H. Evans. Director's qualification, £1,000 in Shares of any class. *Solicitor*—Alfred R. Gery. *Auditors*—Hays, Akers & Hays. *Bankers*—London City and Midland Bank, Limited. *General Manager*—Ernest Webb. *Secretary*—Robert Love.

Here again, the bulk of the information is no personal data. However, under Officials appear the names of natural persons.

[182] 1900, page 131.

Example c

Figure 3: German Yearbook, Aktienführer[183]



Dortmunder Ritterbrauerei
Aktiengesellschaft

Sitz: (21b) Dortmund, Rheinische Straße 49/51

Fernruf: Sa.-Nr. 3 43 45 - 49

Vorstand: Dr. Wilhelm Ahl, Dortmund, Vors.; Dipl.-Kfm. Kurt Hildebrandt, Dortmund; Dipl.-Br.-Ing. Kurt Buettner, Dortmund, stellv.; Dr. Willibald Günther, Dortmund, stellv.; Josef Wagener, Dortmund, stellv.

Aufsichtsrat: Hans Rinn, Hamburg, Vors.; Dr. Felix Eckhardt, Dortmund, stellv. Vors.; Willi Daume, Dortmund; Dipl.-Br.-Ing. Otto Schnitter, Hamburg; Arbeitnehmervertreter: Karl Reiter, Dortmund; Bruno Seltenheim, Dortmund

Gründung: 1889

Tätigkeitsgebiet: Erzeugung von Bier, unter- und obergärig, alkoholfreien Getränken, Eis; Nebenprodukteverwertung im eigenen Betrieb und durch Verkauf.

Beteiligungen: Glückauf-Brauerei AG, Gelsenkirchen Kapital: DM 1 750 000.- (46,5 %) Dividenden ab 1955: 9, 10, 11, 13, 14, 12 %

Brauerei Westfalia Gebr. Hagedorn & Comp. O. H., Münster (Westf.) Kapital: DM 475 000.- (100 %)

Grundstücks-Verwertungs-GmbH, Dortmund Kapital: DM 20 000.- (100 %)

Geschäftsjahr: Kalenderjahr

Stimmrecht d. Aktien i. d. H.-V.: Je nom. DM 100.- = 1 Stimme

Zahlstellen: Gesellschaftskasse; Dresdner Bank AG; Bankhaus Wolff & Co. KG; sämtl. Dortmund; Hermann Lampe KG; Dresdner Bank AG; beide Bielefeld; Bank für Brau-Industrie, Frankfurt (M); Dresdner Bank AG, Düsseldorf, Frankfurt (M) und Hamburg; Bank für Handel und Industrie AG, Berlin

Grundkapital: DM 14 400 000.- Umstellung 10:6 auf DM 4 779 000.- durch H.-V. v. 29. 5. 1951. Lt. H.-V. v. 21. 11. 1955 Erhöhung auf DM 7 200 000.-. Lt. H.-V. v. 31. 5. 1960 Erhöhung aus Gesellschaftsmitteln auf DM 14 400 000.-.

Börsennotiz: Düsseldorf, Berlin und Frankfurt/M (amtl.)

Wertpapier-Kenn-Nr.: 554900

Stückelung: 12 950 Inh.-St.-Akt. zu je DM 1 000.- 1 500 Inh.-St.-Akt. zu je DM 500.- 7 000 Inh.-St.-Akt. zu je DM 100.-

Großaktionäre: Dresdner Bank AG, Frankfurt/M (50,2 %); Bankhaus Wolff & Co. KG, Dortmund (33 %)

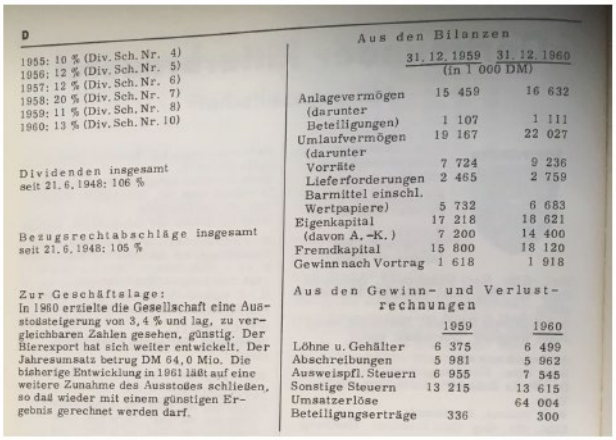
Aktienkurse (Düsseldorf):

ultimo	1948	35 %
"	1949	60 %
"	1950	56 %
"	1951	81,5 %
"	1952	66 %
"	1953	175 % +)
"	1954	400 %
"	1955	350 %
"	1956	375 %
"	1957	480 %
"	1958	690 %
"	1959	1 500 %
"	1960	1 000 %
29. Sept.	1961	746 %

+) ab 15. 12. 1953 Kurs für DM-Nennwert

Dividenden auf Stammaktien: II/1948/49 u. 1949/50: 0 % 1950/51: 5 % (Div. Sch. Nr. 55) 1951/52: 5 % (Div. Sch. Nr. 56) 1952/53: 7 % (Div. Sch. Nr. 1) 1953 (1. 10.-31. 12.): 2 % (Div. Sch. Nr. 1) 1954: 9 % (Div. Sch. Nr. 2)

Fields: (1) Name; (2) Registered address (*Sitz*); (3) Telephone number (*Fernruf*); (4) Board of directors (*Vorstand*); (5) Supervisory board (*Aufsichtsrat*); (6): Year of incorporation (*Gründung*); (7) Activities (*Tätigkeitsgebiet*); (8) Participations on other companies (*Beteiligungen*); (9) Fiscal year (*Geschäftsjahr*); (10) Payment offices (*Zahlstellen*); (11) Capital and details on capital operations (*Grundkapital*); (12) Exchanges where securities are listed (*Börsennotiz*); (13) Identification number of securities (*Wertpapier-Kenn-Nr.*); (14) Nominal value (*Stückelung*); (15) Large shareholders (*Grossaktionäre*); (16) End-of-year quotations (*Aktienkurse*); (17) Annual dividends (*Dividenden auf Stammaktien*)



D

1955: 10 % (Div. Sch. Nr. 4) 1956: 12 % (Div. Sch. Nr. 5) 1957: 12 % (Div. Sch. Nr. 6) 1958: 20 % (Div. Sch. Nr. 7) 1959: 11 % (Div. Sch. Nr. 8) 1960: 13 % (Div. Sch. Nr. 10)

Dividenden insgesamt seit 21. 6. 1948: 106 %

Bezugsrechtabschläge insgesamt seit 21. 6. 1948: 105 %

Zur Geschäftslage: In 1960 erzielte die Gesellschaft eine Ausstoßsteigerung von 3,4 % und lag, zu vergleichbaren Zahlen gesehen, günstig. Der Bierexport hat sich weiter entwickelt. Der Jahresumsatz betrug DM 64,0 Mio. Die bisherige Entwicklung in 1961 läßt auf eine weitere Zunahme des Ausstoßes schließen, so daß wieder mit einem günstigen Ergebnis gerechnet werden darf.

Aus den Bilanzen

	31. 12. 1959	31. 12. 1960
	(in 1 000 DM)	
Anlagevermögen	15 459	16 632
(darunter Beteiligungen)	1 107	1 111
Umlaufvermögen	19 167	22 027
(darunter Vorräte	7 724	9 236
Lieferforderungen	2 465	2 759
Barmittel einschl. Wertpapiere)	5 732	6 683
Eigenkapital	17 218	18 621
(davon A.-K.)	7 200	14 400
Fremdkapital	15 800	18 120
Gewinn nach Vortrag	1 618	1 918

Aus den Gewinn- und Verlustrechnungen

	1959	1960
Löhne u. Gehälter	6 375	6 499
Abschreibungen	5 981	5 962
Ausweispfl. Steuern	6 955	7 545
Sonstige Steuern	13 215	13 615
Umsatzerlöse		64 004
Beteiligungserträge	336	300

Fields: (17) Annual dividends (continued); (18) Total dividends (*Dividenden*): (19) Total subscription rights (*Bezugsrechtabschläge*); (20) Report on the current situation (*Zur Geschäftslage*); (21) Balance sheets (*Bilanzen*); (22) Profit-and-loss accounts (*Gewinn- und Verlustrechnungen*)

Almost no personal data are given save for the executive board and the supervisory board of the stock corporation.

6.2.4. The Personal Data of Deceased Persons

a) Foundation and Evolution

The definition of personal data in Article 4(1) GDPR does not elaborate on the question of whether the data of a deceased person are to be considered personal data, or in other words: whether a deceased person is a "data subject" in the meaning of the GDPR. This topic is not a new one in data protection law; it has already been discussed under the EU Data Protection Directive 95/46/EC.[184] At that time, more diverse interpretations may have existed due to greater leeway for national law. In Germany an intensive debate had been conducted on the direct application of the data protection rules on personal data referring to a deceased person.[185]

However, already the Article 29 Working party (WP29) – the European Data Protection Board's (EDPB)[186] predecessor – issued an opinion on the concept of personal data in 2007.[187] It stated that the term "natural person" in the EU Data Protection Directive 95/46/EC meant "natural living person".[188] Even if the EDPB has formally endorsed (only) the recommendations and opinions of the Article 29 Working party,[189] which were issued after the enactment of the GDPR in 2016, opinions issued prior to that date, as the opinion on the term "natural person", are still an important tool for the interpretation and application of the GDPR. In general terms the Board supports this view in acknowledging the continuity of the work provided by its predecessor.[190]

b) Present Understanding

The GDPR has kept the understanding expressed in Opinion 4/2007 (WP 136) which is supported by Recital 27, sentence 1 GDPR: "This Regulation does not apply to the personal data of deceased persons." Moreover, in regard of data processing for archiving purposes the Regulation specifically

[183] 1962, pages 119-120.
[184] For reference to the Directive, see footnote 80.
[185] For an overview, see *Haase,* Datenschutzrechtliche Frage des Personenbezugs, 2015, page 94.
[186] For more details about these institutions, see Section 6(6.9)(6.9.2).
[187] *Article 29 Data Protection Working Party*, Opinion 4/2007 on the concept of personal data, WP 136, Adopted on 20th June, to be recovered under: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
[188] *Article 29 Data Protection Working Party*, Opinion 4/2007 (WP 136), page 22: "Information relating to dead individuals is therefore in principle not to be considered as personal data subject to the rules of the Directive, as the dead are no longer natural persons in civil law"; downloaded from the WP 29's archives on 17 December 2020: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf; for more details see Section 0(7.1).
[189] The WP 29's papers are still available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613101. The EDPB provides a general link on its website: https://edpb.europa.eu/our-work-tools/article-29-working-party_en.
[190] Endorsement 1/2018, https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

reminds that it should not apply to deceased persons.[191] The same holds for historical research purposes.[192] This is especially noteworthy for EURHISFIRM.

Since this legal reasoning hinges crucially on recitals of an EU legislative act,[193] a clarification of the character of such a recital appears to be necessary. A recital is not formally part of the legal norms enacted. It is a peculiarity of the EU that the recitals are published in the same document as the enacted provisions. This leads quite often to an erroneous legal reasoning as if they were binding norms. The legal character of recitals and enacted norms has to be strictly differentiated. Also the GDPR made this clear by the introduction of the actual text of the provisions of the Regulation (or any other legal act of the EU) after the recitals, and preceded by the words "have adopted this regulation" (directive etc.). Recitals contain information on the motives and understanding of the EU legislators. They are, in this regard, helpful for the interpretation and application of the legal act in question but not binding.

As a result, it would be safe to assume that the substantive rules of the GDPR are not applicable for data relating to a deceased person.[194]

(17) Guideline for EURHISFIRM

The substantive rules of the GDPR are not applicable for data relating to a deceased persons with the result that much of the information processed by EURHISFIRM does not have to comply with the rules of the Regulation.

At least for the examples presented in Section 6(6.2)(6.2.3)(b), this should be the case.

c) Space for Member State's Regulation?

Recital 27 allows, however, in its sentence 2, explicitly national rules in the domain of the GDPR treating the deceased: "Member States may provide for rules regarding the processing of personal data of deceased persons." Since recitals are not part of the actual, formal legal act of "regulation", they cannot contain any opening clauses. Recital 27 should therefore not be called an opening clause. It merely points out the EU legislators' understanding of the term "personal data". As data referring to deceased persons were not within the material scope of Directive 95/46/EC GDPR, EU Member States were allowed to adopt national provisions regulating the handling of the data of the deceased.[195]

---

[191] Recital 158 GDPR sentence 1.
[192] Recital 160 GDPR sentence 2.
[193] In general, falsely translated into German as "*Erwägungsgrund*".
[194] *Gola,* in: Gola, 2018, Article 4 margin number 26; *Klabunde*, in: Ehmann/Selmayr, 2018, Article 4 margin number 13; *Johannes*, in: Roßnagel, 2018, §7 margin numbers 201, 235; *Schwartmann/Mühlenbeck*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, 2020, Article 4 No 1 margin number 16; *Klar/Kühling,* in: Kühling/Buchner, 2020, Article 4 Nr. 1 GDPR margin number 5; *Schild,* in: Wolff /Brink, Beck Online Kommentar Datenschutzrecht, 2020, Article 4 margin number 11; *Karg*, in: Simitis/Hornung/Spiecker, 2019, Article 4 margin number 39: "*Die Anwendbarkeit der DSGVO auf die Informationen einer Person enden mit dem Tod dieser Person; Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 226.
[195] *WP 29*, Opinion 4/2007, page 22: "And fourthly, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46/EC to areas not included in the scope

The GDPR is, however, considerably more comprehensive than the old Directive. It could well be argued that the Regulation encompasses all aspects of the protection of privacy and personal data. As a codification of a complete subject matter it would – contrary to the legislative intention expressed in Recital 27, sentence 2 – be exhaustive and would not allow diverging legislation of the Member States as regards deceased persons. The national law may provide for an extension of data protection. Even if there is no opening clause in the strict sense of the word, it would be advisable to derive from the recital that the framers of the GDPR clearly intended to leave this power to national legislation. It can be assumed that here is one of the (rare) cases where the GDPR is not exhaustive and leaves room for Member States' regulation.[196] The GDPR does not even oblige them "to provide in their legislation special rules for the processing and protecting of personal data of the deceased at their discretion."[197] Details of the national law on this matter are outlined in Sections 0(7.1).

d) Inheritance of Individual Rights under the GDPR?

Another question is whether the heirs of deceased persons inherit the decedents' data subject's rights under the GDPR (right to access, right to erasure, right to restrict processing activities). The result is open. But even if this were the case, the application of the GDPR could not go on forever and – more important for EURHISFIRM – these individual rights could only apply to data processing activities that took place while the deceased was still alive[198] since the GDPR covers only data of living natural persons. There would be no inheritable data subject's rights regarding processing activities taking place after a person's death. For the vast majority of the data processed by EURHISFIRM this would be the case.

(18) Guideline for EURHISFIRM

Even if personal data might be processed by EURHISFIRM, almost all of it will take place after the death of the concerned person. Then, the GDPR is not relevant. Notwithstanding the open question whether individual rights derived from the Regulation are inheritable, the answer will likewise not be relevant for EURHISFIRM since the processing does not take place during the life of the concerned person. This holds specifically for data processing for archiving or historical purposes.

6.3. Material Scope

6.3.1. Principle

The material scope of the protection by the Regulation is quite wide since It encompasses not only the processing of the data "wholly or partly by automated means" but also non-automated means if the personal data "form part of a filing system or are intended to form part of a filing system" (Article 2(1)

thereof provided that no other provision of Community law precludes it, as the ECJ has recalled [reference 16]. It is possible that some national legislator may decide to extend the provisions of national data protection law to some aspects", referring to the Judgment of the European Court of Justice C-101/2001 of 06/11/2003 (*Lindqvist*), margin number 98; *Schwartmann/Mühlenbeck*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, 2020, Article 4 No 1 margin number 16, only with reference to recital 37 without reasoning.

[196] See *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 226: "leaving the issue of post-mortem personal data protection to the discretion of the EU Member States … provides them with unlimited discretion.".

[197] *Ibid.*

[198] *Ziebarth,* in: Sydow DSGVO Article 4 at margin number 11.

GDPR). Hence, even a handwritten note-card can fulfill this requirement if it is made to be included in a collection of note-cards which are sorted following a guiding principle. In view of the danger that personal data sent to a third country will be compromised by authorities, Article 2(1) and (2) GDPR must be interpreted as meaning that that regulation applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.[199]

Processing is defined in Article 4(2) GDPR as "any operation or set of operations which is performed on personal data, whether or not by automated means". From this wide definition follows that, in principle, any use or handling of personal data is covered, "no matter how intensive or long" they are actually processed.[200]

EURHISFIRM will meet these conditions.

(19) Guideline for EURHISFIRM

Designing EURHISFIRM has to respect that the work on it or by it will have to be considered as processing of data in the sense of the Regulation.

6.3.2. Exceptions to the Material Scope

The Regulation provides for some exceptions in Article 2(2). It does not apply to the following processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The activities in the context of EURHISFIRM do not fulfill any of those requirements. In particular, neither the referred Member State activities nor purely personal or household activities are existent. Chapter 2 of Title V TEU concerns common foreign and security policy. The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties also do not fall into the domain of EURHISFIRM.

[199] CJEU case C-311/18 *Schrems II*, ruling 1.
[200] *Rücker,* in: Rücker/Kugler, 2018, margin number 52.

6.4. Personal Scope

6.4.1. Principle

a) Controller or Processor

The main bodies bound by the rules of the GDPR are the "controller" and the "processor".

Controller is defined "as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" (Article 4(7) GDPR).

A Processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Article 4(8) GDPR).

The differentiation between controllers and processors is considered to be essential for determining the responsibilities under the GDPR.[201]

In any case, a group can be a controller irrespective of its precise legal setup as far as it has *determining influence* on the data processing. A consortium suffices.[202]

b) Determining Influence

The attribution of the power to determine "purposes and means" of the data processing is decisive. It may be installed by law or by way of factual influence. Contractual arrangements may also play a significant role. A "joint determination" is also possible and leads to joint responsibilities. This is a likely situation according to the setup of EURHISFIRM as a working infrastructure. In effect, the question has to be decided on a case-by-case basis.[203]

Only if EURHISFIRM infrastructure can and will be installed as a mere platform with no influence on content, comparable to a telecommunication company as ISP, used by various researchers who solely decide ways and means of the processing, will it not necessarily have to be judged as a controller.

6.4.2. Application

If the future EU research infrastructure EURHISFIRM is set up as an entity which collects information from various sources, formats them and distributes them to researchers, it would have to be considered a controller in the meaning of the GDPR.

(20) Guideline for EURHISFIRM

Most likely EURHISFIRM will have to be judged as a controller in the meaning of the GDPR and would be responsible for the lawful processing of the personal data.

[201] *Rücker,* in: Rücker/Kugler, 2018 margin number 121.
[202] *Rücker,* in: Rücker/Kugler, 2018 margin number 122.
[203] *Rücker,* in: Rücker/Kugler, 2018 margin numbers 123, 127, 129.

6.5. Territorial Scope

6.5.1. Principle

For assessing the territorial application of the Regulation three different constellations have to be distinguished. They all result in applicability of the Regulation (Article 3 GDPR):

1. processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not;
2. processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union;
3. processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

In condensed words, the Regulation is applicable if

- either the entity controlling the data processing or the entity doing the actual processing is established in the EU or
- the data subject resides in the EU (under certain circumstances) or
- the controlling entity is established in a place where Member State law applies by virtue of public international law.

6.5.2. Application

Irrespective of the precise legal structure of EURHISFIRM it would have to be considered to fall under the territorial applicability of the Regulation. For the period of designing and setting up the infrastructure either the entity as such is the controller or the participating institutions. In view of the participants from the UK the third indent would probably govern depending on the precise regulation coming up. After EURHISFIRM has been set up as a research infrastructure of the EU it will most likely fall under the first indent. Since EURHISFIRM is designed to be set up for the territory of the EU the first indent will also govern if the property of controller is attributed to the users of the infrastructure regardless of its legal status.

(21) Guideline for EURHISFIRM

EURHISFIRM falls under the territorial applicability of the GDPR.

6.6. General Principles for the Processing of Personal Data

6.6.1. Foundation

Article 5(1) GDPR restates the fundamental principles for the collecting and processing of personal data developed over the years by the case law, some of the national statutes and the preceding data protection directive:

- Lawfulness, fairness and transparency (lit. a)
- Purpose limitation (lit. b);
- Data minimisation (lit. c);
- Accuracy (lit. d);
- Storage limitation (lit. e)
- Integrity and confidentiality (lit. f)

In addition, the controller is responsible for and must be able to demonstrate compliance with these requirements (accountability) (Article 5(2) GDPR).

(22) Guideline for EURHISFIRM

As far as personal data of a living natural person are processed within the research infrastructure EURHISFIRM this has to be performed in compliance with the basic principles laid down in Article 5 GDPR: Lawfulness, fairness and transparency (lit. a), purpose limitation (lit. b), data minimisation (lit. c), accuracy (lit. d), storage limitation (lit. e), integrity and confidentiality (lit. f) and accountability (paragraph 2).

6.6.2. Purpose Limitation

a) The Necessary Specification of Purposes

Personal data shall only “be collected for specified, explicit and legitimate purposes". A similar provision can already be found in Article 5 lit. b ECHR and rudimentarily in Article 8(2) sentence 1 CFR. Already at its collection, the processing of personal data shall be restricted. The specification may take place in any form but has to be sufficiently concrete to be intelligible both for the affected person and the supervisory authority.[204] “Improving users’ experience”, “marketing purposes” or “future research”, for example, are not sufficient.[205]

The data must not be processed further on “in a manner that is incompatible with those purposes”, Article 5(1) lit. b. The initial purposes “adhere” to the data from the beginning and govern the future

[204] *Herbst,* in: Kühling/Buchner, 2020, Article 5 GDPR margin number 35.
[205] *Article 29 Working Party*, Opinion 03/2013 on purpose limitation, WP 203. 2/4/2013, 16; *Heberlein*, in: Ehmann/Selmayr, 2018, Article 6 margin number 9: not even the more specific term “scientific research” is judged to be insufficient.

scope of lawful processing. They play an important role in assessing the "lawfulness of the controller's and processor's activities; not only if and at the time a change of purposes takes place.[206]

From this follows that a differentiation between a very first processing operation, the collection of data, and all other subsequent processing operations has to be observed.[207] Further processing within the meaning of the GDPR has to be understood as any processing of data following the initial collection, irrespective of whether for the purposes initially specified or for any other purpose.[208]

b) Presumed Compatibility

The GDPR provides, however, a specific relaxation relevant for the set up and working of EURHISFIRM: It explicitly rules in Article 5(1) lit. b GDPR that the "further processing" of personal data "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes" and not contrary to the principle of "purpose limitation". This exception can be characterised as an "assumed compatibility".[209] The term research has to be understood very broadly in scope[210] but has to fulfil rather strict requirements in view of its quality and the applied scientific methods. Details are debated in the legal literature.[211] These requirements should not pose any problem for EURHISFIRM, at least not at the present stage.

The diverging regulation between archiving purposes and the other purposes suggest that the latter are considered by the law as always lying in the public interest.[212] Nevertheless, high quality standards of the research have to be fulfilled.[213]

Since EURHISFIRM is planned to be a scientific research infrastructure also serving historical or statistical research, it can be assumed that it may further process personal data initially collected in a lawful way but for other purposes. This implies that it is not necessary to research and examine the initial purposes the data were collected for.

However, not only the specific safeguards and derogations of Article 89 GDPR have to be observed[214] but also the requirement of a sufficient legal basis irrespective of the presumed compliance. At the

[206] *Ibid.*, 21; *Voigt/von dem Busche*, GDPR, 2017, 4.1.2; in part dissenting *Herbst,* in: Kühling/Buchner, 2020, Article 5 GDPR, margin number 40. Another problem is the questionable need for a new legal basis in that case, see for the debate: *ibid.,* at margin numbers 49 and 49a.
[207] *Dienst,* in: Rücker/Kugler, 2018, margin number 283.
[208] See *Dienst,* in: Rücker/Kugler, 2018, margin number 284, but with the – not convincing – constraint: "additional purposes".
[209] *Dienst,* in: Rücker/Kugler, 2018, margin number 286; *Herbst,* in: Kühling/Buchner, 2020, Article 5 GDPR margin number 50: fiction of compatibility.
[210] *Johannes,* in: Roßnagel, 2018, § 7 margin number 246.
[211] See for details *Raum*, in: Ehmann/Selmayr, 2018, Article 89 margin number 25, differentiating between primary and secondary research and emphasizing in this context that the GDPR is not applicable for deceased persons (at margin number 27).
[212] In favour: *Dienst,* in: Rücker/Kugler, 2018, margin number 288.
[213] *Herbst,* in: Kühling/Buchner, 2020, Article 5 GDPR margin number 52.
[214] For details see Section 6(6.8)(6.8.1).

framing stage of the Regulation, this was not clear but it now appears to be the prevailing interpretation.[215]

(23) Guideline for EURHISFIRM

In principle, the activities of EURHISFIRM are affected by the GDPR as far as data related to living natural persons are concerned but exceptions and derogations apply and ease to quite some extent the working of the research infrastructure in view of the purpose the data were initially collected for.

6.7. Prerequisites for a Lawful Processing of Personal Data

The overarching principle of the GDPR for the processing of personal data is that any processing activity is forbidden unless it is justified by law.[216] In the terminology of German public law it can be characterised as prohibition under the reservation of a permission.[217]

6.7.1 Permission by consent or by the law

The processing of personal data needs a specific legal ground. It can only be lawful if covered by either the data subject's consent (Article 6(1) lit. a GDPR) or by permission of the law (Article 6(1) lit. b-f).[218]

Consent is only valid if it is given by an "informed" person. This pre-requisite is closely tied to the limitations derived from the necessary specification of purposes.[219] Consent, no matter which way expressed, will not play a significant role in the context of EURHISFIRM. The vast bulk of the collected and processed data stems from numerous, often unknown sources. Also a permission by any of the exceptions in Article 9(2) GDPR[220] can be construed. Hence EURHISFIRM will have to rely on one of the permissions provided for by the Regulation itself or "ceded" specifications by the Member State's law.

Lit. b und d of Article 6(1) GDPR are on the face of it not fulfilled. Lit. e, "processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller", might serve as a basis for EURHISFIRM. Also lit. f "legitimate interests" would have to be considered too.

a) Public interest or exercise of official authority

Principles

Subparagraph e of Article 6(1) GDPR follows a functional approach[221] but does not as such contain a permission. The function has to be derived from a different legal source. Although a legal obligation of

[215] See *Herbst,* in: Kühling/Buchner, 2020, Article 5 GDPR margin number 54.
[216] *Voigt/von dem Busche*, GDPR, 2017, 1.2.2; for the critique on this principle see *Buchner/Petri,* in: Kühling/Buchner, 2020, Article 6 GDPR margin number 14.
[217] *Buchner/Petri,* in: Kühling/Buchner, 2020, Article 6 GDPR margin number 11.
[218] The terminology ("legitimation") used by *Dienst,* in: Rücker/Kugler, 2018, at margin numbers 364 et seq., 429 et seq., is highly questionable.
[219] See Section 6(6.6)(6.6.2) above; *Heberlein*, in: Ehmann/Selmayr, 2018, Article 6 margin number 9.
[220] Although the provision explicitly adresses only special categories of personal data and permisses their processing it can be applied on "normal" data by a conclusion *a maiora ad minus*, see *Schmitt/Resch,* Juris die Monatszeitschrift, 4 (2020), page 137
[221] *Buchner/Petri,* in: Kühling/Buchner, 2020, Article 6 GDPR margin number 111.

the controller or the processor to do the processing is not required,[222] a legal basis has to be laid down by Union law or Member State law to which the controller is subject: Article 6(3) GDPR. From this follows the actual permission.[223] This clause also specifies requirements which have to be fulfilled by such a basis:

- The processing shall be *necessary for the performance* of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- The legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia:
  - the general conditions governing the lawfulness of processing by the controller;
  - the types of data which are subject to the processing;
  - the data subjects concerned; the entities to which, and the purposes for which, the personal data may be disclosed;
  - the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX.
- The Union or the Member State law shall meet an objective of public interest and be *proportionate* to the legitimate aim pursued.

The Union or Member State law can also determine "whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so (…) by private law, such as a professional association."[224] In essence, it does not have to be an entity which commands sovereign powers.[225] In principle, a public law research entity could qualify. This includes at least public institutions of higher education (universities). What is essential is that providing access to the research infrastructure would lie in the public interest.[226]

Application

EURHISFIRM as a platform and its working can hardly be judged as processing "in the exercise of official authority" even if it should be set up as a public law entity and the participants are part of a public law research institution, unless it is explicitly empowered by the law of Member States fulfilling the pre-requisites described before. This – unlikely – case has to be scrutinised separately.

More likely is the case that the processing of personal data carried out by EURHISFIRM lies "in the public interest". It would not be totally unreasonable to take the legal view that establishing a research

[222] See *Dienst,* in: Rücker/Kugler, 2018, margin number 388.
[223] *Roßnagel,* in: Simitis/Hornung/Spiecker, 2019, Article 6 GDPR margin number 79; *Schmitt/Resch,* Juris Die Monatsschrift (JM) 4(2020), page 135.
[224] Recital 45 GDPR.
[225] Ambiguous *Buchner/Petri,* in: Kühling/Buchner, 2020, Article 6 GDPR margin numbers 114, 117.
[226] *Buchner/Petri,* in: Kühling/Buchner, 2020, Article 6 GDPR margin number 127.

platform and using it for strictly research purposes is in the "public interest" as far as access to the research community is granted. If the caveats described before are additionally observed, it could be judged as lawful processing of personal data. In specific, it would need a basis in Union or Member State law as well.

(24) Guideline for EURHISFIRM

Processing of personal data by EURHISFIRM could be lawful according to Article 6(1) lit. e GDPR if a suitable basis for the processing is provided in Union law or Member State law. This could be the respective laws on universities or their charters granted by the states.

b) Legitimate Interests

Principles

"Legitimate interests" could exist for example "where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller." The relationship between the controller and the data subject and its expectations play an important role in assessing the existence of a legitimate interest. A crucial question has to be "whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place."[227]

If a research institution is functioning as a "public authority" it has to be taken into account that "it is for the legislator to provide by law for the legal basis for such authorities to process personal data". "That legal basis should not apply to the processing by public authorities in the performance of their tasks."[228]

The legislative motives provide further examples for "legitimate interests", specifically: preventing fraud and direct marketing purposes. They show how open and vague the term is.

In any case, a balancing of the affected interests is indispensable.[229] The interests and fundamental rights of the data subject could in particular override the interest of the data controller if personal data are processed in circumstances in which data subjects do not reasonably expect further processing. The interests or the fundamental rights and freedoms of the data subject may be "overriding". In this respect, the relaxation of the principle of purpose limitation will be helpful for EURHISFIRM.[230]

Although a general exemption for pseudonymised data was intensively discussed, eventually it was not enacted. Pseudonymisation of the personal data processed could, however, decisively influence the result of the balancing.[231]

---

[227] Recital 47 GDPR.
[228] *Ibid*.
[229] *Buchner/Petri,* in: Kühling/Buchner, 2020, Article 6 GDPR margin numbers 141, 149.
[230] See Section 6(6.6)(6.6.2).
[231] *Buchner/Petri,* in: Kühling/Buchner, 2020, Article 6 GDPR, margin number 154; *Johannes*, in Roßnagel, § 7 margin number 249; see for the concept of pseudonymisation and practical advice: *Watteler/Ebel,*

Application

The "reasonable expectations of data subjects based on their relationship with the controller", proposed by the legislative motives as an important criterion,[232] are of limited direct relevance for EURHISFIRM since it is designed to process *historical* data. In a first step, it can be assumed that at the time of the collection of the data little or no reasonable expectations existed in terms of further processing taking place. It could, however, be imputed in a second step that at the time of the collection of these data the notion of privacy and personal data was quite different. The data subjects were probably aware that e.g. their names would be collected in registers or yearbooks designed for public access or publication in print. Further processing already took place at that time even if it was very limited due to the lack of technical means. At least since the inception of a public trading place (stock exchanges, clearing houses) results were listed and used for further processing by hand. This was one of the objectives for which authorities installed them.

(25) Guideline for EURHISFIRM

Processing of personal data by EURHISFIRM could be lawful according to Article 6(1) lit. f GDPR on the ground of a "legitimate interest".

6.7.2 Organisational Requirements for Controllers and Processors

a) Records of Processing Activities

Controllers and processors have to implement records of their processing activities that will allow supervisory authorities to monitor whether the rules of the GDPR have been obeyed (Article 30(1) and (2) GDPR). These records have to include:

- Name and contact details
- Purpose of the processing
- Description of the categories of data subjects and of personal data
- Categories of data recipients
- Transfers of personal data to third countries
- General description of security measures according to Article 32(1) GDPR[233]

Forschungsdatenmanagement, 2019, pages 64-68. The techniques for anonymiszation and pseudonymisation are described on pages 69-74.

[232] Recital 47 GDPR.

[233] See for a comprehensive collection of guidelines of national supervisory authorities *Müthlein*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, 2020, Article 30 margin number 100.

A data protection officer may keep the records.[234] If they are thoroughly maintained they will permit the entities affected to prove their compliance with the law.[235]

b) Security of Processing

The GDPR requires - as already the old Data Protection Directive - technical and organisational measures to ensure appropriate security in processing of personal data (Article 32(1) GDPR). The term "security" is used in a specific way and can be considered as part of the more encompassing concept of data protection. An absolute security is almost impossible to reach; at least would be be very costly to achieve. This is why the provision requires only a level of security "appropriate" to the risk. It gives as examples:

a) Pseudonymisation and encryption
b) Ability to ensure confidentiality, integrity, availability and resilience of processing systems
c) Ability to restore availability and acces in a timely manner
d) A process for regularly testing, assessing and evaluating the effectiveness of the measures taken.

This list is neither conclusive[236] nor a minimum standard.[237]

From the legislative motives it can be derived which specific risks the controller or processor should regard and mitigate. With the objective to "ensure an appropriate level of security, including confidentiality" the "the state of the art and the costs of implementation" shall be balanced with "the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage."[238]

In addition, the outcome of impact assessments[239] should be taken into account when determining the concrete measures. Where the assessment "indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation", a consultation of the supervisory authority according Article 36 GDPR should take place prior to the processing.[240]

Beyond this, the law does not prescribe details of the measures to be employed. Since the given specifications are still quite vague considerable space is left for interpretation. The result of the

[234] *Article 29 Working Party,* Data protection officers Guidelines on Data Protection Officers ('DPO'), WP243 rev.01, endorsed by the EDPB on 25 May 2018, endorsement 1/2018, https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf; *Müthlein*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, 2020, Article 30 margin number 30.
[235] *Voigt/von dem Busche*, GDPR, 2017, 1.2.1.
[236] *Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, 2020, Article 32 margin number 27.
[237] Ibid., at 28.
[238] GDPR recital 83.
[239] See infra d).
[240] GDPR recital 84.

balancing is open[241] and can only exclude obvious failures or complete inactions. In any case it would be advisable to fix in writing the aspects considered and a reason for the decision.

For EURHISFIRM might be important that the controller is responsible even if the processing is in total executed by someone else like scholars who use the research infrastructure.[242] If EURHISFIRM will eventually only provide services and does neither control the processing nor orders it the responsibility will be limited to the part it can control.[243]

c) Designation of a Data Protection Officer

According to Article 37(1) GDPR certain institutions are obliged to designate a Data Protection Officer (DPO). This obligation exists:

- if the processing is carried out by a public authority or body (irrespective of what data is being processed)
- if the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale
- if the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.[244]

Union or Member State law may furthermore require the designation of DPOs in other situations. Finally, even if the designation of a DPO is not mandatory, organisations may sometimes find it useful to designate a DPO on a voluntary basis.[245]

From this follows that *private* entities are obliged to designate a Data Protection Officer if their core activities consist of regular and systematic monitoring of data subjects or of processing special categories of personal data on a large scale.[246] EURHISFIRM might eventually process data on a large scale but they are mainly not personal data and – foreseeably – not of a special category. Moreover, so far EURHISFIRM is not organised as a private entity. If that changes in the future a new evaluation will have to take place.

Public authorities and other (public) bodies are obliged to designate a DPO irrespective whether the afore-mentioned conditions. It can be well argued that EURHISFIRM at the moment is not (yet) such an entity but rather a contractual cooperation of various bodies within the framework of a project. Hence, it would not fulfil the requirement of the norm. In addition, it can be assumed that the

[241] *Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, 2020, Article 32 margin number 81.
[242] *Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, 2020, Article 32 margin number 23.
[243] See *ibid.,* at 25; critical *Spiecker,* in: Simitis/Hornung/Spiecker, 2019, margin number 15.
[244] Annex 5 to: *Article 29 Data Protection Working Party*, Guidelines on Data Protection Officers (‚DPOs') 16/EN WP 243 rev.01, 13 December 2016, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.
[245] *Ibid*.
[246] *Voigt/von dem Busche*, GDPR, 2017, 1.2.1.

(potential) obligations of the participating entities of EURHISFIRM are met by the respective Data Protection Officers of the entities they belong to.

All this needs, however, a new assessment as soon as the institutional setup of EURHISFIRM is altered.

d) Data Protection Impact Assessment

Only if the intended processing activity "is likely to result in a high risk to the rights and freedoms of the data subjects must entities carry out a preventive Data Protection Impact Assessment to identify appropriate measures for mitigating the risks to data protection."[247] At the designing stage it is not visible but might have to be taken into account at the working stage, but only if actually personal data will be processed on a large scale.

6.8. Derogations and Exemptions for Archives and Scientific Research

As a general rule,[248] it has to be underlined that the protection of privacy and personal data in general and the GDPR in specific do not intend to obstruct research. On the contrary, the primary law of the EU stresses explicitly the importance of research and technological development. It obliges in Article 179 TFEU all institutions and organs of the EU to enhance and support them:[249]

> *Article 178*
>
> 1. The Union shall have the objective of strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely, and encouraging it to become more competitive, including in its industry, while promoting all the research activities deemed necessary by virtue of other Chapters of the Treaties.
>
> 2. For this purpose the Union shall, throughout the Union, encourage undertakings, including small and medium-sized undertakings, research centres and universities in their research and technological development activities of high quality; it shall support their efforts to cooperate with one another, aiming, notably, at permitting researchers to cooperate freely across borders and at enabling undertakings to exploit the internal market potential to the full, in particular through the opening-up of national public contracts, the definition of common standards and the removal of legal and fiscal obstacles to that cooperation.

The GDPR acknowledges this obligation which has to be decisive for the interpretation of its rules. In the course of the legislative procedures the wording of the relevant clauses in the draft of the GDPR were several times altered in order to comply with this obligation. The proposal of the Commission had been extremely restrictive[250] which is not surprising in view of the well organized and very well funded special interests with science-hostile convictions.

National legislation has used the space ceded by Article 6(2) and (3) GDPR, like Germany in section 27 BDSG and the state legislatures in the university acts.

[247] *Voigt/von dem Busche*, GDPR 2017, 1.2.1.
[248] Recitals 26, 33, Article 6(1) lit. e GDPR.
[249] *Raum*, in: Ehmann/Selmayr, 2018, Article 89 margin number 6.
[250] For details of the legislative history see *ibid,* at margin numbers 12-16

EURHISFIRM is situated at the core of these considerations.

6.8.1. Limitation of the Application

It has already been mentioned[251] that the GDPR contains an explicit limitation ("presumed compatibility") when it provides in Article 5(1) lit. b that the "further processing" of personal data "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall (…) not be considered to be incompatible with the initial purposes". Since EURHISFIRM is planned as a research infrastructure it can be assumed that it may further process personal data going beyond the initial (lawful) purpose. However, the specific safeguards and derogations of Article 89 GDPR have to be observed.

(26) Guideline for EURHISFIRM

EURHISFIRM may process personal data beyond the initial purpose they were collected for, subject to the safeguards and derogations specified in Article 89 GDPR, however.

a) Pseudonymisation

Article 89(1), sentence 2 GDPR provides that the safeguard and derogations "shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation." As a general rule it provides explicitly for one such measure "Pseudonymisation, provided that those purposes can be fulfilled in that manner".[252] It further reduces the exemption by additionally ordering that, where "those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."

From this follows that a complete anonymisation is not required.[253] Pseudonymisation may by sufficient, pursuant to Article 89(1), sentence 3 GDPR.[254] It means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".[255]

b) Derogations for Research and Statistical Purposes

In addition, following Article 89(2) GDPR Union or Member State law may provide for derogation from several rights on information and access to personal data where personal data are processed for scientific or historical research purposes or statistical purposes: Article 15 GDPR: Right of access by the data subject, Article 16 GDPR: Right to rectification, Article 18 GDPR: Right to restriction of processing

[251] Section 6(6.2)(6.6.2)(b).
[252] It can also be assessed as a "presumed compatibility".
[253] This follows from Recital 26 sentence 4 GDPR, see also *Watteler/Ebel,* Forschungsdatenmanagement, 2019, pages 65 et seq. and Section 6.2.3(a) above.
[254] Recitals 28, 29, 75, 78, 85 GDPR, specifically for research: Recital 156. Explicitly mentioned in Article 6(4) lit. e, Article 32(1).
[255] Definition in Article 4(5).

and Article 21: Right to object. Such derogation is, however, only admissible in so far as the rights "are likely to render impossible or seriously impair the achievement of the specific purposes and such derogations are necessary for the fulfilment of those purposes".

c) Derogations for Archiving Purposes

Derogations are also allowed where personal data are processed for archiving purposes in the public interest. This relates to the rights of Articles 15, 16, 18, 19, 20 and 21 GDPR subject to similar caveats as for the derogations for research and statistical purposes.

d) Summary

Derogations by Union or Member State law from certain rights are allowed without prejudice for scientific or historical research as well as for statistical purposes. Processing for archival purposes has to be in the public interest. From this differentiation can be gathered that the law considers the research purposes always to be in the public interest.[256]

6.8.2. Exemptions and Exceptions from Specific Requirements

In general, a *notification* of the data subject is prescribed by Article 14 GDPR. A relaxation is, however, granted in paragraph 5 subparagraph b of this provision for the processing for archiving purposes in the public interest or research and statistical purposes. Under the condition that "such information proves impossible or would involve disproportionate effort" the obligation is reduced to "measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available". The same would hold "in so far as the obligation referred to in paragraph 1 of this Article [i.e. Article 14 GDPR] is likely to render impossible or seriously impair the achievement of the objectives of that processing".

Data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered according to the legislative motives "as cases where the provision of information to the data subject would involve a disproportionate effort", especially when "taking the number of data subjects, the age of the data and any appropriate safeguards adopted … into consideration".[257]

The *Article 29 Data Protection Working Party* gives the following example which would fit well to EURHISFIRM's situation:

> Historical researchers seeking to trace lineage based on surnames indirectly obtain a large dataset relating to 20,000 data subjects. However, the dataset was collected 50 years ago, has not been updated since, and does not contain any contact details. Given the size of the database and more particularly, the age of the data, it would involve disproportionate effort for the researchers to try to trace the data subjects individually in order to provide them with Article 14 information.

[256] See Section 6(6.8)(6.8.1)(b).
[257] Recital 62.

In the rare case that personal data of a living person is processed by EURHISFIRM a notification on the "publicly available"[258] homepage can be considered as sufficient.[259]

Similar alleviations hold for the *right to erasure* in Article 17(3) subparagraph d GDPR, and *right to object* in Article 21(6) GDPR.

6.9. Institutional Provisions

6.9.1. Member-State Level

The GDPR contains in Chapter VI unusually detailed provisions for the installation and powers of independent supervisory authorities on the national level. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR. Its objective is to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.[260]

6.9.2. EU Level

a) European Data Protection Board

The national EU data protection supervisory authorities work together in the European Data Protection Board (EDPB). The EDPB is an independent body with legal personality responsible for ensuring the consistent application of the General Data Protection Regulation (GDPR). The EDPB succeeds the Article 29 Working party set up under Article 29 of Directive 95/46/EC. It is composed of the Member States' data protection authorities and the European Data Protection Supervisor (EDPS).[261] The Article 29 Working Party had adopted guidelines, opinions and recommendations on various aspects of the GDPR, contributing thus to the consistent application of the GDPR. It consulted interested parties where appropriate.

Since the harmonization between the GDPR and the ePrivacy directive has not been accomplished frictions in the application of the substantial rules and the working of the institutions are not rare.[262] The EDPB has attempted to mitigate the problems by issuing a detailed opinion on the interplay in May 2019.[263]

The EDPB has formally endorsed only the recommendations and opinions of the Article 29 Working party,[264] which were issued after the enactment of the GDPR in 2016:

---

[258] Article 14 paragraph 5 subparagraph b sentence 2 GDPR.
[259] *Article 29 Data Protection Working Party*, WP260 rev.01 of 11/04/2018, page 31 margin number 64.
[260] Article 51(1) GDPR.
[261] Details on the members can be found on the homepage of the EDPB: https://edpb.europa.eu/about-edpb/board/members_en.
[262] See Section 3(3.2)(3.2.2)(d) above.
[263] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.
[264] The WP 29's papers are still available under: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613101. The EDPB provides a general link on its website: https://edpb.europa.eu/our-work-tools/article-29-working-party_en.

1. Guidelines on consent under Regulation 2016/679, WP259 rev.01

2. Guidelines on transparency under Regulation 2016/679, WP260 rev.01

3. Automated individual decision-making and profiling Guidelines on Automated individual decisionmaking and Profiling for the purposes of Regulation 2016/679, WP251rev.01

4. Personal data breach notification Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01

5. The right to data portability Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01

6. Data protection impact assessment Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01

7. Data protection officers Guidelines on Data Protection Officers ('DPO'), WP243 rev.01

8. Lead supervisory authority Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01

9. Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR

10. Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP 263 rev.01

11. Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264

12. Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265

13. Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01

14. Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01

15. Adequacy Referential, WP 254 rev.01

16. Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253.[265]

Opinions issued prior to that date are, however, still an important tool for the interpretation and application of the GDPR. In general terms the Board is committed to maintaining continuity with the

[265] https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf .

work provided by its predecessor.[266] The EDPB publishes general information on the GDPR on its website, including guidelines, recommendations and best practices.[267]

GDPR: Guidelines, Recommendations, Best Practices

- Guidelines 10/2020 on restrictions under Article 23 GDPR - version for public consultation
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - version for public consultation
- Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 - version for public consultation
- Guidelines 08/2020 on the targeting of social media users - version for public consultation
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR - version for public consultation
- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR - Adopted after public consultation
- Guidelines 05/2020 on consent under Regulation 2016/679
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak
- Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak
- Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies - version adopted after public consultation
- Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications - version for public consultation
- Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) - version adopted after public consultation
- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default - version adopted after public consultation
- Guidelines 3/2019 on processing of personal data through video devices - Adopted after public consultation

[266] *Ibid*.

[267] https://edpb.europa.eu/our-work-tools/general-guidance_en. Other documents are available under: https://edpb.europa.eu/other-documents_en.

- Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725)
- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation
- Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation
- Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - version adopted after public consultation
- Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation
- Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679
- Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation

b) Data Protection Officers

As already mentioned, another institutional trait covered by Article 37(1) GDPR is the obligation for certain undertakings and institutions to designate a Data Protection Officer (DPO).[268]

6.10. Scope of Application

Due to its wide material scope the GDPR applies to all matters concerning the protection of fundamental rights and freedoms vis-à- vis the processing of personal data, however, with a far-reaching exception: All processing of personal data which are "subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons" is *not* covered. This is also the reason why the EU legislator stipulated in 2016 that "Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation."[269] This is, however, not yet accomplished.[270]

7. Specific Problems

7.1. The Protection of the Deceased Revisited

The problem of the protection of deceased persons' data has already been discussed in Section 6(6.2)(6.2.4) but it deserves some more in-depth reflections since it is to a large extent such data that EURHISFIRM will process. But there are no clear-cut results. A recent law review article came

[268] See for more details, Chapter 6(6.7)(6.7.2)(b), above.
[269] Recital 173 GDPR.
[270] See Section 3(3.2)(3.2.2)(d) above.

to the result that "there is not any developed unified approach, how to solve the legal issues of post-mortem personal data protection in the framework of the EU."[271]

From the political economy approach the personal data of the dead are more and more recognized as a marketable good and exploiting the online death has become a a new "business" model.[272]

7.1.1. Foundations

When determining whether data pertain to deceased persons or to living persons, it should be kept in mind that even if data ostensibly refer to a deceased person, they may indirectly also indicate one or more living persons. This may be the case with health data. Information on a genetic disorder may not only refer to the deceased, it may also include a reference to the health of his or her relatives. Such a rare case might happen but is not perceivable as regards the specific data processed by EURHISFIRM.

Even though personal data on deceased persons do not fall into the scope of the GDPR, they may also be covered by other legal provisions, such as those treating medical privilege (doctor's confidentiality), tax secret (*Steuergeheimnis*) or social secret (*Sozialgeheimnis)*. In German law, data collected and edited by the federal or state statistics offices may also be covered by specific secrecy requirements.[273] It is, however, likely that these aspects will likewise not come into play for EURHISFIRM. Specific rules on the protection of intellectual property or works of art contain in general an extension of protection beyond the death of the creator.[274] This does not at all hold for the rules on data protection.

In the legal literature is hence summarized "that there is a situation when neither the EU primary (the EU Charter of the Fundamental Rights) or secondary law (in particular, the GDPR), nor the European Convention on Human Rights, nor the case law of both European Supranational Courts provide for post-mortem data protection in the EU.[275]

Some aspects of a deceased person's personality rights (*Persönlichkeitsrechte*) might, however, persist and be protected under constitutional and civil law even if they are not captured by the specific data protection regime of the EU. Some authors even go beyond this and attempt to construe from *interests* of the dead genuine *rights*[276]: "Recognition of posthumous legal rights gives the dead significant moral standing within our legal system, as would be expected if lawmakers are driven by a desire to treat the dead with dignity."[277]

[271] *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 227 et seq., 230, explicating the different proposals to solve the problems. But they are almost completely only advice to lawmakers.
[272] *Öhmanl/Floridi,* Minds & Machines, vol. 27 (2017), pages 640 et seq.
[273] See *Taeger/Gabel*, DSGO, Article 4 margin number 19.
[274] As regards protection of the copyright in literary works, this is explicated in detail in the report on WP 3.1. and is not part of this report.
[275] *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 238.
[276] *Smolensky,* Hofstra Law Review, vol. 37 no 3 (2009), page 764, adopting an "Interest Theory approach to rights".
[277] *Ibid.*

7.1.2. The Lacking Explicit Regulation

Like the GDPR, both the EU Charter on Fundamental Rights and the European Convention on Human Rights contain no word on the "possibility of their application to post-mortem privacy protection".[278]

7.1.3. The Case Law of the European Supranational Courts

The CJEU did not yet issue a judgment directly addressing the question of a post-mortem protection. In its *Lundquist* case[279] it touched it indirectly by indicating that the Member States would be free to regulate the question themselves. Although the judgment was still on the rules of the old Data Protection Directive its main rulings can be carried over to the GDPR.

In contrast to the CJEU, the ECtHR had to consider the application of human rights to deceased persons in a variety of cases. In general the Court held that Article 8 ECHR should only be applied to living persons.[280] In specific, it stated "it would stretch the reasoning in this case-law too far to hold in a case like the present one that DNA testing on a corpse constituted interference with Article 8 rights of the deceased's estate".[281]

7.1.4. Data Protection Law of the Member States

Since in respect of the personal data of deceased persons the Member States have space for their own rules a wide variety of solutions exists: (i) In one group of Member States (Denmark, Hungary) the protection is in principle extended for a specified period after the death of a person. (ii) In a second group (Slovakia, Estonia, Bulgaria) the consent of interested persons, like close relatives or heirs, is the decisive criterion. (iii) The third group of Member States (Spain, Italy), France) "provides for interested persons to realize the right to be forgotten post-mortem, if this is not contrary to the law or was not prohibited by the data subject themselves during their lifetime".[282]

In Spain it is Article 3 of the Data Protection Act which "provides that the heirs of a deceased person have the right to access, delete and correct the relevant data from the data controllers and processors, unless such deletion or correction was prohibited by the deceased person or by applicable law." Under similar provisions, in Italy the data protection rights of sections 15-22 GDPR can be activated for the dead by "activated by the data subject who is interested in protection, by their agent or for family reasons worthy of protection ("representative"), except for cases established by law, or where the data subject has expressly prohibited this by a written application provided or communicated to the data controller." A unique approach is taken by the French law which provides "for the possibility for data subjects to establish instructions for the management of their personal data after death in the law on data protection and the rules for exercising their right to a digital death."[283]

A more in-depth analysis of the national rules has to be reserved to additional research in a project of its own when details of the institutional setup of EURHISFIRM in its working stage are known.

---

[278] *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 233.
[279] CJEU C-101/01 of 6/11/2003 *Lindquist,* at margin number 98.
[280] See for references *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 233.
[281] *The Estate Of Kresten Filtenborg Mortensen v. Denmark*, App. no. 1338/03 of 15 May 2006.
[282] The following information and grouping builds on the work of *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), pages 230 et seq.
[283] *Ibid.,* with references.

7.1.5. Protection of the Deceased outside the Data Protection Rules

A protection of information referring to deceased persons might follow from fundamental rights enshrined in constitutional law or the case-law of the ordinary courts in private law cases. It is, however, a misconception to contrast categorically the German judicature against the French because of an alleged monistic approach of the German law.[284]

a) The German Constitutional Law

At least in Germany, the (general) personality right [*allgemeines Persönlichkeitsrecht*], derived from Article 2(1) of the Basic Law[285] in conjunction with Article 1(1) Basic Law (human dignity) protects the inner personal sphere.[286] The general personality right complements as an "unnamed" civil right [*unbenanntes Freiheitsrecht*] the special ("named") civil rights [*benannte Freiheitsrechte*] which protect the constituent elements of the personality as well.[287] The right of personality development [*Recht auf freie Entfaltung der Persönlichkeit*] and human dignity guarantee everyone an autonomous sphere of conduct of life in private [*autonomen Bereich privater Lebensgestaltung*], in which "he can develop and uphold his individuality" [*in dem er seine Individualität entwickeln und wahren kann*].[288]

> Moreover, in its molding [*Ausformung*] as a right of informational self-determination [*Recht der informationellen Selbstbestimmung*] it [the general personality right] grants everyone the capacity to decide himself about the divulgence and use of his personal data (cf. BVerfGE 130, 1 [35]) and, in addition, to decide when and to what extent facts of his personal life is disclosed (cf. BVerfGE 103, 21 [33]).[289]

A lasting effect of the general personality right, including the right of informational self-determination, on which most of the statutory protection of privacy and personal data is built, has to be negated because bearer of this right can only be a living person. With that person's death her protection expires.[290]

---

[284] *Edwards/Harbinja,* Cardozo Arts & Entertainement Law Journal, vol. 32 no 1 (2013), page 104. The explications and classifications in foreign law review articles on the German legal situation are not specific enough; see for example *Edwards/Harbinja,* Cardozo Arts & Entertainement Law Journal, vol. 32 no 1 (2013), page 101, 103 et seq., following the widely spread but weird attempt to separate the legal world into "Common Law" and "Civilian Systems"; often named "Civil Law Systems" instead; similarly *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 237.

[285] *Grundgesetz*, the German federal constitution.

[286] BVerfGE 121, 69 (90); 146, 1 margin number 102.

[287] See BVerfGE 79, 256 (268); 119, 1 (24), 146, 1 margin number 102 (13/6/2017).

[288] BVerfGE 146, 1 margin number 102: *"Das Recht auf freie Entfaltung der Persönlichkeit und die Menschenwürde sichern jedem Einzelnen einen autonomen Bereich privater Lebensgestaltung, in dem er seine Individualität entwickeln und wahren kann (vgl. BVerfGE 79, 256 [268])."*

[289] BVerfGE 146, 1 margin number 102: *"Ferner gibt es [das allgemeine Persönlichkeitsrecht] dem Einzelnen in seiner Ausformung als Recht der informationellen Selbstbestimmung die Befugnis, selbst über die Preisgabe und Verwendung persönlicher Daten (vgl. BVerfGE 130,1 [35]) sowie darüber zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (vgl. BVerfGE 103, 21 [33])."*

[290] BVerfGE 146, 1 margin number 103: "*Das Fortwirken des Persönlichkeitsrechts nach dem Tode ist zu verneinen, weil Träger dieses Grundrechts nur die lebende Person ist. Mit ihrem Tode erlischt der Schutz aus diesem Grundrecht."* See also: BVerfGE 30, 173 (194); BVerfG-K, NVwZ 2008, 550; and from the literature e.g. *Jarass,* in: Jarass/Pieroth, GG, Article 2 margin number 51.

A constitutional *post mortem* protection can only be derived from Article 1(1) Basic Law, the clause on human dignity. But also human dignity ends according to the German doctrine with death. Only some very limited obligations may have a lasting effect (*nachwirkende Schutzpflichten*).[291] The existence of such obligations in general is, however, questioned in the legal literature and their scope is dubious.[292] In any case, the claim for fundamental respect derived from Article 1(1) Basic Law only protects against gross degradation and vilification. Such information will most likely not be processed by EURHISFIRM. Any defamation can easily be avoided.

(27) Guideline for EURHISFIRM

In case personal data should be processed by EURHISFIRM, for all practical purposes it may be assumed from the German perspective that no restrictions arising from fundamental rights are relevant as far as the data refer to deceased persons. The forbidden vilification is not to be expected and can easily be avoided.

b) German Private Law

Even before the constitutional (general) personality right was developed, the case law of the highest civil court in Germany accepted the protection of personality rights by private (civil) law.[293] It was extended in certain cases to a *post mortem* protection and comprised monetary and intangible components,[294] since it was originally not based on Article 1 Basic Law and did not contain aspects of the protection of personal data.[295]

c) National Law of non-German Member States

Several Member States, like Germany, Ireland and Cyprus, have employed their discretion[296] to abstain from adopting "any rules for processing and protecting personal data of the deceased". Sweden has explicitly such a protection.[297] A general scrutiny of the national law outside the specific data protection rules in view of the protection of deceased persons beyond Germany has to be left to further (comparative) research as well.

[291] BVerfGE 30, 173 (194); BVerfG-K, NVwZ 2008, 550; *Höfling,* in: Sachs, GG, Article 1 margin numbers 63 et seq.; *Jarass*, in: Jarass/Pieroth, GG, Article 2 margin number 51.
[292] *Huber,* in: HGR II, § 49 margin number 24; not sufficiently recognized by *Edwards/Harbinja,* Cardozo Arts & Entertainement Law Journal, vol. 32 no 1 (2013), page 101
[293] *Gola,* in: Gola, 2018, Article 4 margin number 24.
[294] BGH [highest German civil court], NJW 2007, 684 (685); *Gola,* in: Gola, 2018, Article 4 margin number 27; correctly explicated by *Edwards/Harbinja,* Cardozo Arts & Entertainement Law Journal, vol. 32 no 1 (2013), page 104 but erroneously confounded with the constitutional law judicature of the GFCC; similarly *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 237.
[295] *Karg*, in: Simitis/Hornung/Spiecker DSGVO, Article 4 margin number 39.
[296] See Section 6(6.2)(6.2.4) above.
[297] *Hamuľák/Kocharyan/Kerikmäe*, CYIL Vol. 11 (2020), page 226.

7.2. Exemptions for a Prevailing Interest of the General Weal

7.2.1. EU law

In contrast to some proposals during the legislative process, Article 89 GDPR does *not* contain a general exemption in favour of data processing by archives or scientific research.[298] The protection of personal data may, however, come into conflict with rules that guarantee the freedom of expression and information, including journalistic, academic and artistic or literary expression. In specific, scientific research is protected by Article 13 FRC and constitutional law of the Member States. They are held to harmonise these freedoms with the GDPR: Processing of personal data solely for journalistic purposes, or for the purposes of academic expression

> should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. (…) Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights.[299]

The Regulation provides some guidelines for designing these exemptions and derogations which have, however, more the character of mere reminders of the aspects to be considered than strict normative orders: "Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations." More substance has the following statement that, because of the importance of the freedom of expression for a democratic society, notions relating to that freedom should be interpreted "broadly".[300]

Moreover, in regard of data processing for archiving purposes the Regulation specifically reiterates that it should not apply to deceased persons.[301] The same holds for historical research purposes.[302] This is especially noteworthy for EURHISFIRM.

In case of divergence, the GDPR recommends: "Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply."[303]

To qualify for an exemption, these requirements have to be met:

- Prevailing interest of the general weal

[298] *Schwartmann/Mühlenbeck/Wybitul*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, 2020, Article 89 margin numbers 2, 7 et seq.
[299] Recital 153 GDPR.
[300] *Ibid*.
[301] Recital 158 GDPR sentence 1; see also *Pauly,* in: Paal/Pauly, Article 89 GDPR margin number 9.
[302] Recital 160 GDPR sentence 2.
[303] *Ibid*.

- Statutory basis
- Proportionality
- No intrusion into the inner private sphere
- Respecting the essence of the fundamental rights, Article 52(1), sentence 1 CFR.[304]

The GDPR does not intend to obstruct research or the freedom of expression, or free access to information. It leaves the balancing in principle to the national law of the Member States. Pseudonymisation or anonymisation might suffice in many cases.[305]

7.2.2. German Constitutional Law

The German Federal Constitutional Court has acknowledged already in early decisions that the Basic Law grants "the individual citizen an inviolable realm of a private conduct of life" which "is shielded from all intrusions on behalf of public authorities".[306] This general personality right has been molded into a "right of informational self-determination" *(Grundrecht auf informationelle Selbstbestimmung)* and a "fundamental right of data protection" *(Datenschutzgrundrecht)*. But these rights are not granted absolutely.

As concerns the conflict between the protection of privacy and personal data on the one side and other protected rights, the German Federal Constitutional Court has held that the citizen "has to tolerate measures which are implemented in the prevailing interest of the general weal on a statutory basis respecting the principle of proportionality, provided that they do not impair the inviolable realm of the private conduct of life".[307] This is relevant for public archives as a source of information[308] and especially for the academic freedom enshrined in Article 5(3) of the Basic Law.

To qualify for an exemption, these requirements have to be met:

- Statutory basis,
- Prevailing interest of the general weal,
- Proportionality,
- Intrusion into the inner private sphere only under exceptional circumstances,
- No infringement of the essence of the fundamental rights, Article 52(1), sentence 1 CFR,[309] Article 19(2) Basic Law.

---

[304] CJEU case C-362/14 *Schrems I*, at para 94.
[305] *Pötters,* in: Gola, 2018, Article 89 margin number 10 et seq.
[306] BVerfGE 27, 344 (350); similarly earlier BVerfGE 6, 32 (41): "sphere of private conduct of life"; BVerfGE 27, 1 (6); later BVerfGE 34, 269 (281): "sphere of privacy for each human being".
[307] BVerfGE 89, 69 (84).
[308] Protected by the right of freedom of expression and the right of access to information according to Article 5(1) Basic Law but not only. Other public interests exist.
[309] CJEU case C-362/14 *Schrems I*, at para 94.

7.3. Codes of Conduct

Articles 40, 41 GDPR introduce the instrument of Codes of Conduct. They are to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises (Article 40 Section 1 GDPR).

7.3.1. Scope and Goal

The European Data Protection Board has published Guidelines for Codes of Conduct, where it further explains the scope and goal of Codes of Conduct:

> GDPR codes are voluntary accountability tools which set out specific data protection rules for categories of controllers and processors. They can be a useful and effective accountability tool,[310] providing a detailed description of what is the most appropriate, legal and ethical set of behaviours of a sector. From a data protection viewpoint, codes can therefore operate as a rulebook for controllers and processors who design and implement GDPR-compliant data-processing activities which give operational meaning to the principles of data protection set out in European and National law. (…)
>
> Codes can help controllers and processors to comply with the GDPR by governing areas such as fair and transparent processing, legitimate interests, security and data protection by design and default measures and controller obligations. Codes are accessible to all processing sectors and can be drafted in as narrow or as wide-ranging a manner as is befitting that particular sector, provided that the code contributes to the proper and effective application of the GDPR.[311]

7.3.2. Definition

"Codes of conduct are sets of agreed principles to meet data protection requirements"[312]; or somewhat more detailed: Approved codes of conduct are an aid to the correct application of the requirements of the GDPR for specific categories of users.[313] They are understood as an instrument of self-regulation[314], however, a voluntary one.[315]

---

[310] The presumption of "effective accountability" established by codes of conduct can be questioned with good reasons. Some of the biggest scandals of the recent past were enabled by the application of the widely propagated principle of "regulated self-regulation". The unprecedented collapse, for example, of the German blue-chip stock corporation "Wirecard" was only possible because surveillance was largely delegated to an (underperforming) private entity of "self-regulation" (DPR) and the, in general, competent authorities excused themselves in view of the deficits which were known to insiders that they lost their competence due to the privatisation of surveillance. The relevant "code of conduct" was laughable, and failed in total. Details are still under investigation but lead - after long hesitation - to the resignation of the president of a supervisory agency.

[311] EDPB Guidelines 01/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, page 7 et seq. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf; the "easing of an effective application of the Regulation" is emphasized in the legal literature, see *Paal/Kugler,* in: Paal/Pauly, Article 40 GDPR margin numbers 3, 5, 15.

[312] *Schrey,* in: Rücker/Kugler, 2018, margin number 566.

[313] *Schweinoch,* in: Ehmann/Selmayr, 2018, Article 40 margin number 1.

[314] *Bergt/Pesch,* in: Kühling/Buchner, 2020, Article 40 margin number 8; *Voigt/von dem Busche*, GDPR, 2017, 3.9; *Paal/Kugler,* in: Paal/Pauly, Article 40 GDPR margin number 3.

[315] *Schweinoch,* in: Ehmann/Selmayr, 2018, Article 40 GDPR margin number 1, emphasizing the voluntariness.

7.3.3. Nature and Origin

Where codes of conduct are set up to meet the GDPR's requirement of "fair" processing or "legitimate interests", one could speak of codes of conduct as ethical rules, whereas the requirement of "fair processing" and "legitimate interests" are legal terminology set forth by the GDPR which need to be interpreted in its application. They are not concepts derived outside of statutory law.

Also, the GDPR states that "associations and other bodies representing categories of controller or processors may prepare codes of conduct". In the private sector, these bodies usually are industry bodies such as trade associations for a specific industry sector. In the public sphere, codes of conduct in the science sector are imaginable.

They might have their merits as a form of "privatisation of control". There are, however, drawbacks to this type of a "regulated self-regulation" the GDPR tries to promote. In any case, the circumvention of the constitutionally prescribed process of law making is an imminent danger. Hence it is doubtful whether such codes can be more than mere advice for an interpretation and application of the law which a court of law may notice and then set aside.

7.3.4. Types

There are two different types of codes of conduct: National and transnational codes of conduct. When a code of conduct adopted by a national association in one Member State covers processing activities by its members in several Member States, it will qualify as a transnational code. If, however, an association with a code approved at national level is joined by an international member that conducts cross-border processing, that member could only claim the benefit of the approved code for processing activities in the Member State which approved the code. Mechanisms would need to be put in place to ensure that there is adequate transparency as regards the effective territorial scope of the code.[316]

Transnational codes of conduct approved by a Data Protection Supervisory Authority are published in a register on the European Data Protection Board's website.[317] As of 28 December 2020, only two cross-border codes of conduct have been approved:

1. Autocontrol Codes of Conduct (Asociación para la Autorregulación de la Comunicación Comercial) on Accountability, Advertising.
2. Nederland ICT Codes of Conduct ("Data Pro Code").

7.3.5. Publication

National Data Protection Supervisory Authorities are required to publish national codes of conduct (Article 40 Section 6 GDPR). As these codes of conduct do not relate to processing activities in more

[316] EDPB Guidelines 01/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, page 27, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf.
[317] EDPB Guidelines 01/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, page 20. The EDPB's register is available under: https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en).

than one Member State, there is no legal requirement to publish a national code of conduct in another language than the respective national language.[318]

7.3.6. No Binding Force

The democratic principle requires that only persons may be subject to such rules who have "voice", i.e. can give their view and vote on their adoption, and that no fundamental rights be ceded. This is why the "codes of conduct" in the meaning of the GDPR do not have legally binding effects even if they are approved or declared generally applicable in the Union.[319]

They ease the burden of proof. "Controllers or processors may adhere to those codes to show compliance with data protection law."[320]

(28) Guideline for EURHISFIRM

Codes of conduct have to be researched nationally. Two cross-border codes of conduct have been notified so far: in Spain and the Netherlands.

7.4. Homepage/Survey

Concerning the homepage of EURHISFIRM specific legal rules are in force which are part of the regulation of electronic communication.[321] The rules on electronic communication are not the subject of this report. They have developed into a separate discipline of the law and would require an extensive additional report which would have only marginal relevance for the core questions regarding the objective and working of EURHISFIRM. Notwithstanding, some remarks on the topic might be helpful.

7.4.1. Foundations

In the first place, the rules are designed to secure the working of the technical infrastructure and free, non-discriminatory access to it. But also provisions guaranteeing the privacy of communication by technical and organisational measures belong here.

On a second layer, the access providers are regulated. The main objective of these rules is to promote the working of the single market by enhancing communication. This relates widely to users' rights in mobile electronic communication networks and open access to the internet. A concrete example is the regulation of roaming charges to foster competition and lower the – often prohibitive – costs. Another

[318] Example: LDI NRW: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Verhaltensregeln-_-Code-of-Coduct/Inhalt/Verhaltensregeln-und-Akkreditierung-von-Ueberwachungsstellen-nach-der-DS-GVO/Verzeichnis-genehmigter-Verhaltensregeln-bei-der-LDI-NRW-nach-Art_-40-Absatz-6-DS-GVO.html.

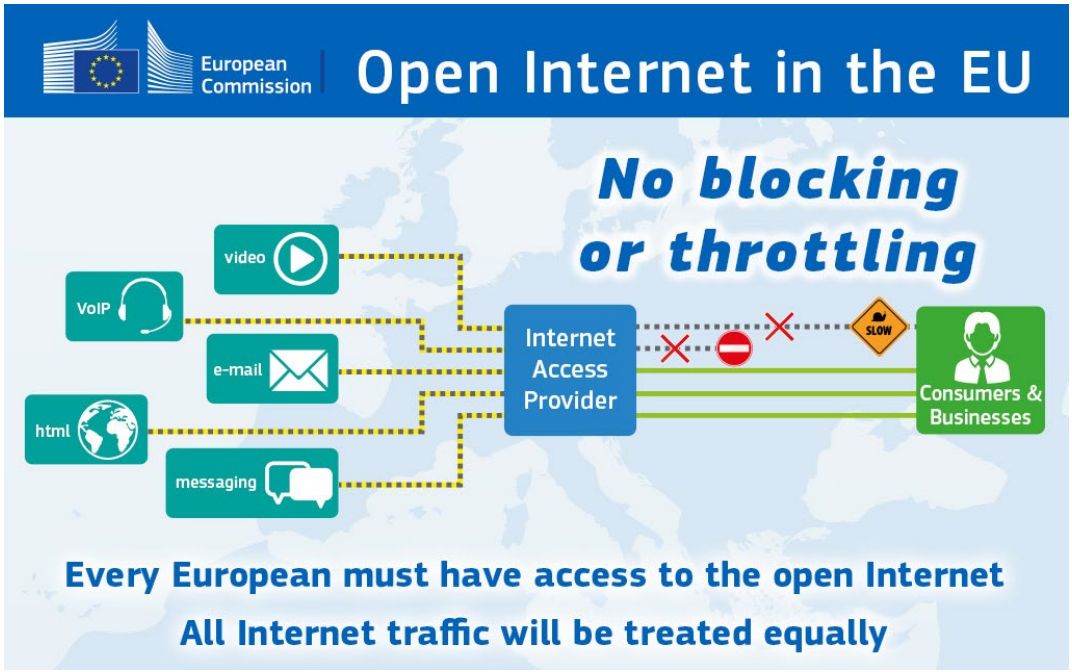
[319] *Bergt/Pesch,* in: Kühling/Buchner, 2020, Article 40 GDPR margin number 8; *Voigt/von dem Busche*, GDPR, 2017, 3.9.2.4; different at 3.9.2.1.

[320] *Schrey,* in: Rücker/Kugler, 2018, margin number 566.

[321] Another topic is the use of internet data, in specific data of the providers, for research, see *Watteler/Ebel,* in: Forschungsdatenmanagement, 2019, pages 63 et seq.

important goal is the equal treatment of all internet traffic.[322] For a visualisation see the following Figure 3, provided by the EU Commission.[323]

Figure 4: Open Internet



On a third layer, the content providers are obliged to follow a specific set of rules set up for the communication via a homepage.

This separation, however, does not rule out that, in principle, the regulation on the protection of privacy and personal data have to be observed when using (electronic) instruments of communication including the internet.[324] Only insofar as specific clauses of the rules on electronic communication take precedence as *lex specialis* they might override the rules on privacy and personal data. This has to be decided case by case since the EU did not succeed in harmonising the two legal regimes as initially intended. The GDPR and its corollaries went into force before a consensus on a general reform of the rules on electronic communication could be reached. The relevant old *ePrivacy directive* is still valid but a consensus on the reform has finally been reached in February 2021.[325] So far, the unresolved

[322] See REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ L 320/1, 16.11.2015.
[323] https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality.
[324] *EDPB,* Opinion 5/2019, pages 11 et seq. Without hesitation, the CJEU has referred to the ePrivacy Directive in conjunction with the GDPR in a recent judgment, case C-673/17 of 1 October 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV* v *Planet49 GmbH,* ECLI:EU:C:2019; for a general assessment of the problem see the opinion of the EDPB of 12 March 2019, Opinion 5/2019, https://edpb.europa.eu/our-work-tools/our-documents/styrelsens-yttrande-art-64/opinion-52019-interplay-between-eprivacy_en.
[325] See above, Section 3(3.2)(3.2.2)(d).

frictions continue to exist. Since according to Article 3 the material scope of the Directive[326] (and the future Regulation) is confined to electronic communication it is only at the margin relevant for EURHISFIRM.

The separation of the subject matters is more strictly observed by the *European Electronic Communications Code*[327] which is clearly only directed at the first two levels.[328] Its subject matter is to establish a "harmonised framework for the regulation of electronic communications networks, electronic communications services, associated facilities and associated services, and certain aspects of terminal equipment. It lays down tasks of national regulatory authorities and, where applicable, of other competent authorities, and establishes a set of procedures to ensure the harmonised application of the regulatory framework throughout the Union."[329] Its aims are to

> (a) implement an internal market in electronic communications networks and services that results in the deployment and take-up of very high capacity networks, sustainable competition, interoperability of electronic communications services, accessibility, security of networks and services and end-user benefits; and to
>
> (b) ensure the provision throughout the Union of good quality, affordable, publicly available services through effective competition and choice, to deal with circumstances in which the needs of end-users, including those with disabilities in order to access the services on an equal basis with others, are not satisfactorily met by the market and to lay down the necessary end-user rights.[330]

The protection of privacy and personal data is recognised but not its objective, Article 1(3)(b). The whole legislative document mentions the GDPR only once. There it reminds that "processing of personal data by electronic communications services, whether as remuneration or otherwise, should comply with Regulation (EU) 2016/679 of the European Parliament and of the Council", the GDPR.[331]

7.4.2. Recently Debated Topics

Some aspects which have evolved into major topics for the legal debate are:

[326] Article 3: "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices".
[327] See above, Section 3(3.2)(3.2.2)(e).
[328] Article 2(1): 'electronic communications network' means transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.
[329] DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code (Recast), OJ of 7/12/2018, L 321/39, Article 1(1).
[330] *Ibid.*, Article 1(2).
[331] *Ibid*., recital 17.

- The responsibility of a platform operator for content provided by users of the platform
- The right or factual power to exclude users
- Privacy and/or data protection statements on the hompage
- The specific problem of user identification and the employment of cookies.

Although these topics are intertwined, for analytical purposes, they should be separated. Save the third indent which might be the most relevant for EURHISFIRM, they are all extremely problematic in the light of fundamental rights even if the transgressions originate from private persons or institutions. In the end, that makes them even more dangerous since judicial control would be easier if the concrete infringements would be state actions. In specific, the freedom of expression, the free access to information, and the due process requirements are severely jeopardized, most recently in the case of the former president of the United States.

a) Privacy Statements

The rules on privacy statements might become relevant for EURHISFIRM but not much of clear legal provisions exist. As a result, many of these statements are a mixture of storytelling, paraphrases of legal norms, wordy unfolding of a company's (institution's) policies, and marketing talk. Many of them try to force the user to cede all her rights by asking for an explicit consent to the lengthy fine print of the owner.[332] If such a lump sum consent, ceding all rights to a part of an oligopoly is valid at the end of the day has to be doubted. As a general rule, derived from other fields of law, it is safe to assume that the longer and the more complicated such a statement is, on which consent is based, the more likely it is that it will be declared void in court.

The EU itself, is hardly a role model in this respect. The privacy statement on the homepage of the Commission for the "EU Login": "One account, many EU services", reproduced as appendix 4, contains little concise legal content. Ironically the EU demands identification before the user can enter the respective homepage; contrary to the elsewhere advocated free access to information. Another example that could have served as role mode is the privacy statement used by EUDAT which is – like EURHISFIRM – a Horizon2020 project, also initiated in view of a European Research Infrastructure. It is reproduced as appendix 5.

b) Cookies

The attempts to install systems of user identification on personal computers are almost as old as their interconnectedness via the world wide web, and since leaving the realm of military and scientific use. When commerce gradually discovered the web in the 1980[ies] the technical means to set cookies were implemented in the operating systems and browsers. This was, of course, always illegal, from the beginning on, and this, without recourse to any (mostly not yet existing) data protection laws. Their potential was grossly underestimated and nobody really cared that an interested person or entity manipulated a foreign computer without the *indispensable* permission. It was widely ignored that this made them globally identifiable by the visited homepage setting the cookie (tracking cookies).

[332] Critical *Heidrich,* c't 18 (2020), page 37.

However, the personal computer was for quite some time not really personal and it was commercially not so interesting to make its use identifiable. This changed over time and is especially relevant since the spread of smart phones which, in fact, are usually only used by one person for the commercially interesting transactions. The potential to make a person – no matter whether anonymous or not – globally identifiable is not only interesting for the authorities but even more for commerce and the emerging so called tech industry.[333] It was one of the most important drivers for their business models and their growth to unanticipated power. Courts and the competent authorities are now much more aware of this almost universal breach of law.

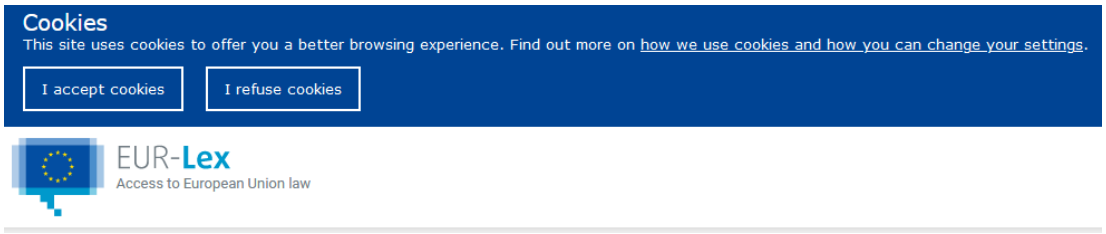
On October 1, 2019 the CJEU decided that a pre-ticked checkbox does not constitute valid consent for cookies – irrespective of whether the information stored in the cookie contains personal data or not. The CJEU further ruled that the information on cookies must include information on the storage period of the cookie and, whether third parties have access to cookies.[334] The judgment is mainly based on Article 5(3) ePrivacy Directive which stipulates: "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent (…)." Since the ePrivacy Directive does not contain further information on how to obtain consent, the CJEU referred to recital 17 of the ePrivacy Directive which states that "consent of a user or subscriber (…) should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC."[335] Cookies are, however, a topic of the GDPR as well.[336]

The judgment of the CJEU had been given as a preliminary ruling of the German *Bundesgerichtshof,* which fully transposed it into the original case in a recent decision using an EU law friendly interpretation of the relevant clause of the German law (Section 15(3) TMG).[337]

The users of this instrument still go out of their way to circumvent these decisions and try to conceal their true objectives in pages and pages of fine print and propaganda like “we value your privacy” and “we provide you a better user experience”. The handling by Alphabet (google, youtube etc) is a telling example for this and does for certain not fulfill the requirements of EU-law. A positive counter-example is in this respect the EU-Commission:

[333] See for technical details *Kleinz,* c’t 18 (2020), pages 24-28.
[334] CJEU case C-673/17 of 1 October 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV* v *Planet49 GmbH,* ECLI:EU:C:2019:801.
[335] *Ibid*, at margin number 50.
[336] *EDPB*, Opinion 5/2019, page 11 et seq., with more references and details.
[337] BGH, Urteil vom 28. Mai 2020 [judgment of 28 May 2020] – case: I ZR 7/16 - *Cookie-Einwilligung II,* Neue Juristische Wochenschrift (NJW 2020), page 2540.

Figure 5: Cookies



The widely used exemption for allegedly "technically necessary" cookies is highly questionable since Article 5(3) ePrivacy Directive requires that "any technical storage or access" is allowed without explicit consent only "for the sole purpose of carrying out the transmission". The transmission is according to the specifications of the http protocol technically possible without setting *any* cookies, just somewhat uncomfortable. If at all, only session cookies could be considered as technically necessary.

7.4.3. Application

Conducting a survey might not in the least affect the protection of personal data. The general rules about the obligations when processing the obtained data have to be respected. Specific requirements will have to be fulfilled if the actual processing is performed by an outside party, a "processor" in the terminology of the GDPR.

a) Personal Data

The homepage uses the term "personally identifiable information" which surely is a legal term and probably intended to fulfill the requirements of the GDPR. However, the Regulation uses the term "personal data" as encompassing.[338]

b) ZOHO as Processor?

EURHISFIRM is the designer and operator of the "Business & Governance Model Survey" and thus a controller within the meaning of the GDPR. In conducting the survey it uses the servicer ZOHO. It is, however, not altogether clear whether the notices given on the homepage of EURHISFIRM are intended to be the full information required by Article 13 GDPR[339] or a reference to the data protection information of ZOHO.[340] No matter what ZOHO provides or promises, the controller in the sense of Article 4 No 7 GDPR is EURHISFIRM and it thus remains fully responsible for the compliance of the processor according to the provisions of Article 28 GDPR. In case of doubt it has to be assumed that a mere reference to the "GDPR compliance" of the servicer is not sufficient even if the functionality provided there is as such prudent and advisable.

[338] See Section 6(6.2).
[339] An (approved) model for a data protection declaration on homepages can be found here: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Datenschutzhinweise-Websites/Muster-Datenschutzhinweise-Websites---Juli-2019.pdf [in German]; for more practical details see *Solmecke/Kocatepe,* DSGV, 2018, pages 94-108, 189-237.
[340] https://www.zoho.com/privacy.html.

Specifically, the declaration of ZOHO on third-party service providers could prove to be problematic:

> *Third-party service providers*: We may need to share your personal information and aggregated or de-identified information with third-party service providers that we engage, such as marketing and advertising partners, event organizers, web analytics providers and payment processors. These service providers are authorized to use your personal information only as necessary to provide these services to us.[341]

"Marketing and advertising partners" might be too vague. It is not clear whether this affects only the creator of a survey or also the participants. Moreover it has to be taken into account that ZOHO might now have to be considered a third country processor, at least from the perspective of the EU law.[342]

c) Use of Cookies

If the survey sets cookies, the participants have to be informed about this fact and must be given the choice to deny consent to all not technically indispensable cookies. This option should be preset and easy to find irrespective of whether something like a "technically indispensable cookie" really exists or if it is just a matter of comfort or correct programming.

d) Users' Rights

The right to rectification according to Article 16 GDPR should be mentioned.

8. Executive Summary

(1) Data protection and data security should be distinguished.

(2) Ethical rules in the genuine sense of the world must not play a significant role in the context of EURHISFIRM.

(3) In essence, it should be derived from Article 8 ECHR that privacy is in principle protected as a human right but is, in principle, confined to living persons.

(4) The GDPR is exhaustive and conclusive, thus foreclosing national regulations in the field of data protection and privacy unless explicitly permitted. In the relevant subject matters, the national law of Member States is limited to a marginal role.

(5) The statutory rules of the Member States are a source of law, to be observed by EU-RHISFIRM but with a greatly diminished importance because of the primacy of the comprehensive EU harmonisation by the GDPR, which is directly binding law in all Member States.

[341] Privacy Policy, Part I, Who we share information with.
[342] "Cloud services firm Zoho to shift U.S. headquarters", t*he Hindu* of *15 July 2019,* ISSN 0971-751X, r*etrieved 22 July 2019.*

(6) For EURHISFIRM it is, however, important to have an opening for Member State rules in view of the protection of deceased natural persons.

(7) In the UK, during the transition period the same legal rules continue to be in force which govern the set-up and working of EURHISFIRM.

(8) Before the end of the transition period on 31 December 2020 an agreement on the future relationship between the EU and the UK has been reached and will provide for the relevant legal regime.

(9) Most legal rules on the protection of personal data and privacy remain in force. In any case Article 8 of the Withdrawal Agreement has to be taken into account.

(10) EURHISFIRM has to assume that the GDPR uses the term "personal data" in a very wide sense covering any information relating to an identified or identifiable natural person. The name of a person in conjunction with their telephone number or information about their working conditions or hobbies suffices. This holds true as well for IP addresses.

(11) As data on the financial situation of firms or prices in a stock exchange usually contain little or no information related to natural persons, the significance of legal rules protecting them is very limited for EURHISFIRM. This holds true especially for stock exchange reports. However, as far as natural persons behind them or acting on behalf of them are identifiable they might be relevant.

(12) When processing personal data in the Union the following fundamental rules derived from Article 8 CFR, reiterated and elaborated by the secondary law of the Union, are crucial:

- Specification of the purpose(s),
- Consent of the person concerned or legitimate basis laid down by (statutory) law,
- Right to access to the data,
- Right to rectification.

(13) The practical relevance of Article 8 CFR for the working of EURHISFIRM is limited.

(14) The GDPR does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of

the legal person and the contact details of the legal person. Information collected from stock exchanges will hence be "safe" from legal rules protecting personal data. Information collected from stock exchanges will be "safe" from legal rules protecting personal data.

(15) The substantive rules of the GDPR are not applicable for data relating to a deceased person with the result that much of the information processed by EURHISFIRM does not have to comply with the rules of the Regulation. At least for the examples presented in Section 6(6.2)(6.2.3)(b), this should be the case.

(16) Even if personal data might be processed by EURHISFIRM, almost all of it will take place after the death of the concerned person. Then, the GDPR is not relevant. Notwithstanding the open question whether individual rights derived from the Regulation are inheritable, the answer will not be relevant for EURHISFIRM either since the processing does not take place during the life of the concerned person. This holds true specifically for data processing for archiving or historical purposes.

(17) In case personal data should be processed by EURHISFIRM, for all practical purposes it may be assumed from the German perspective that no restrictions arising from fundamental rights are relevant as far as the data refer to deceased persons. A forbidden defamation can be avoided.

(18) When designing EURHISFIRM one has to consider that the work on it or by it will have to be considered as processing in the sense of the GDPR.

(19) Most likely EURHISFIRM will have to be judged as a controller within the meaning of the GDPR and would be responsible for the lawful processing of the personal data.

(20) EURHISFIRM falls under the territorial applicability of the GDPR.

(21) As far as personal data of a living natural person are processed within the research infrastructure EURHISFIRM this has to be performed in compliance with the basic principles laid down in Article 5 GDPR: Lawfulness, fairness and transparency (lit. a), purpose limitation (lit. b), data minimisation (lit. c), accuracy (lit. d), storage limitation (lit. e), Integrity and confidentiality (lit. f) and accountability (paragraph 2). But derogations apply.

(22) In principle, the activities of EURHISFIRM are affected by the GDPR as far as data related to living natural persons are concerned, but exceptions and derogations apply, and these ease

to quite some extent the working of the research infrastructure in view of the purpose the data were initially collected for.

(23) Processing of personal data by EURHISFIRM could be lawful according to Article 6(1) lit. e GDPR if a suitable basis for the processing is provided in Union law or Member State law. This could be the respective acts on universities or their charters granted by the states.

(24) Processing of personal data by EURHISFIRM could be lawful according to Article 6(1) lit. f GDPR on the ground of a "legitimate interest".

9. List of Court Decisions

9.1. European Court of Human Rights

- Application No 27798/95 of 16/2/2000, *Amann v Switzerland*
- Application No 1338/03 of 15 May 2006, *The Estate Of Kresten Filtenborg Mortensen v. Denmark*
- Application Nos 58170/13, 62322/14, 24960/15 of 13/9/2018, *Big Brother Watch v United Kingdom*

9.2. Court of Justice of the EU[343]

- Case 6/64 of 15/7/1964, *Costa v E.N.E.L.,* ECLI:EU:C:1964:66
- Joined cases C-465/00, C-138/01 and C-139/01, *Court of Audit v Austrian Broadcasting System*, ECR 2003 I-4989
- C-101/01 of 06/11/2003, *Lindqvist*, ECR 2003 I 12971, ECLI:EU:C:2003:596
- C-275/06, *Promusicae*, ECR 2008 I-271
- C-524/06, *Heinz Huber*, ECR 2008 I-9705
- C-301/06, *Ireland v Parliament and Council,* ECR 2009 I-593
- Joined Cases 293 & 594/12 of 8/4/2014, *Digital Rights Ireland v Minister for Commc'n*, E-CLI:EU:C:2014:238.
- C-362/14 of 6/10/2015, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, [*Schrems I*]
- C-582/14 of 19/10/2016, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779
- C-203/15 of 21/12/2016, *Tele2 Sverige* (meta-data retention), ECLI:EU:C:2016:970
- C-434/16 of 20/12/2017, *Nowak,* ECLI:EU:C:20176:994
- C-673/17 of 1/10/2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV* v *Planet49 GmbH,* ECLI:EU:C:2019:801
- C-311/18 of 16/07/2020, *Data Protection Commissioner, Facebook Ireland Ltd., Maximilian Schrems,* ECLI:EU:C:2020:559 [*Schrems II*]

[343] Formerly European Court of Justice (ECJ).

9.3. German Federal Constitutional Court

- BVerfGE 6, 32
- BVerfGE 10, 89
- BVerfGE 15, 235
- BVerfGE 27, 1
- BVerfGE 27, 344
- BVerfGE 30, 173
- BVerfGE 34, 269
- BVerfGE 37, 1
- BVerfGE 38, 281
- BVerfGE 65, 1 (informational self-determination – judgment on census);
- BVerfGE 79, 256
- BVerfGE 89, 69
- BVerfGE 100, 313; 115, 166 (online search)
- BVerfGE 115, 166
- BVerfGE 117, 202
- BVerfGE 118, 168
- BVerfGE 119, 1
- BVerfGE 120, 180
- BVerfGE 120, 274 (protection of information technology)
- BVerfGE 120, 351
- BVerfGE 121, 69
- BVerfGE 128, 1
- BVerfGE 130,1
- BVerfGE 133, 277
- BVerfGE 135, 155
- BVerfGE 136, 194
- BVerfGE 146, 1

- BVerfG-K, NVwZ 2008, 550

9.4. Other Courts

- RG Judgment of 11 April 1901, Case: V1 443100 = 48, 114 (124)

- RGZ 80, 221
- RGZ 150, 1

- BGHZ 17, 327
- BGH, Judgment of 28. Mai 2020 – case: I ZR 7/16 - *Cookie-Einwilligung II,* Neue Juristische Wochenschrift (NJW) 2020, 2540

10. List of References

10.1. Materials

Article 29 Data Protection Working Party, Opinion 4/2007of 20.06.2007 on the concept of personal data (01248/07/EN, WP 136), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203 of 2/4/2013)

Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/67 (WP 260 rev.01 of 29/11/2018, as last Revised and Adopted on 11/04/2018), available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

European Data Protection Board, Legal framework, https://edpb.europa.eu/legal-framework_en

European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities of 22 March 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

10.2. Literature

Brkan, Maja, The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core, 14 European Constitutional Law Review (2018), pages 332-368

Brkan, Maja, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning, German Law Journal (2019), 20, pages 864-883

Custers, Bart/Dechesne, Francien/Sears, Alan M./Tani, Tommaso/van der Hof, Simone, A comparison of data protection legislation and policies across the EU, Computer Law & Security Review 34(2) (2018), pages 234-243, available at: http://www.sciencedirect.com/science/article/pii/S0267364917302856 (accessed: 20 January 2021).

Dreier, Horst, Die "guten Sitten" zwischen Normativität und Faktizität, in: Friedrich Harrer/Heinrich Honsell/Peter Mader (Hrsg.) [editors], Gedächtnisschrift für Theo Mayer-Maly, 2001, pages 141-158

Edwards, Lilian/Harbinja, Edina, Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World, Cardozo Arts & Entertainement Law Journal, vol. 32 no 1 (2013), pages 83-129

Ehmann, Eugen/Selmayr, Martin (Hrsg.) [editors], DS-GVO: Datenschutz-Grundverordnung, 2. Auflage [2nd edition], 2018

Esser, Josef, Einführung in die Grundbegriffe des Rechtes und des Staates, 1949

Frowein, Abraham, Besprechung EuGH, 15. 7. 1964 – Rs. 6/64, Costa/E.N.E.L., RIW/AWD 1964, 258

Gola, Peter (Hrsg.) [ed.], Datenschutz-Grundverordnung, 2. Auflage [2nd edition], 2018

Haase, Datenschutzrechtliche Frage des Personenbezugs, 2015

Hamuľák, Ondrej/Kocharyan, Hovsep/ Kerikmäe, Tanel, The Contemporary Issues of post-mortem Personal Data Protection in the EU after GDPR Entering into Force, Czech Yearbook of Public & Private International Law (CYIL), Vol. 11 (2020), pages 225-238[344]

Hartley, T.C., The Foundations of European Union Law, 8th edition 2014

Hart, H.L.A., The Concept of Law, 1961 (reprinted 1970)

Heidrich, Joerg, Kein Privacy Paradies, c't 18 (2020), pages 36 et seq.

Heidrich, Joerg, In letzter Minute, c't 3 (2021), pages 26 et seq.

Hösle, Vittorio, Die Krise der Gegenwart und die Verantwortung der Philosophie. Transzendentalpragmatik, Letztbegründung, Ethik, 2. Auflage [2nd edition], München, 1994

Huber, Peter Michael, in: Detlef Merten/Hans Jürgen Papier (Hrsg.) [editors], Handbuch der Grundrechte, vol. II § 49, 2006

Jarass, Hans D. and *Pieroth, Bodo,* Grundgesetz für die Bundesrepublik Deutschland, 16. Auflage [15th edition] 2020

Kleinz, Torsten, Targeting, Conversion Rate und SSPs, c't 18 (2020), pages 24-28

Konzelmann, Alexander, Methode landesrechtlicher Rechtsbereinigung, 1997.

Kriele, Martin, Dialektische Prozesse in der Verfassungsgeschichte, in: Joachim Burmeister et alia (Hrsg.) [editors], Verfassungsstaatlichkeit, Festschrift für Klaus Stern zum 65. Geburtstag, 1997, pages 15-28

Kruis, Tobias, Der Anwendungsvorrang des EU-Rechts in Theorie und Praxis, 2013

Kühling, Jürgen/Buchner, Benedikt, Datenschutz-Grundverordnung/BDSG, 3. Auflage [3rd. edition] 2020

Ludwigs, Markus / *Sikora, Patrick,* Der Vorrang des Unionsrecht unter Kontrollvorbehalt des BVerfG, EWS 2016, 121

[344] The author is grateful to *Ondrej Hamuľák* for the swift information on the printed source and the permission for citations.

Mayer-Maly, Theo, Was leisten die guten Sitten, Archiv für Civilistische Praxis (AcP), vol. 194 (1994), pages 105-176

Möllers, Thomas M.J., Legal Methods, 2020

Morgan, Edmund S., Inventing the People, 1988

Müthlein, Thomas (Hrsg.) [editor], Datenschutz-Grundverordnung-General Data Protection Regulation, 3. Auflage [3rd. Edition], 2018

Öhman, Carl/Floridi, Luciano, The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry, Minds & Machines, vol. 27 (2017), pages 639-662

Paal, Boris P./Pauly, Daniel A. (eds.), Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 3. Auflage [3rd edition], 2021

Pechstein, Matthias/Nowak, Carsten/Häde, Ulrich, Frankfurter Kommentar zu EUV, GRC und AEUV, 2017

Pieper, Annemarie, Einführung in die Ethik, München, 1994

Roßnagel, *Alexander* (ed.), Das neue Datenschutzrecht, 2018

Roßnagel, Alexander/Bile, Tamer/Friedewald, Michael/Geminn, Christian/Grigorjew, Olga/Karaboga, Murat/Nebel, Maxi, National implementation of the general data protection regulation, 2018, available at: http://publica.fraunhofer.de/documents/N-481274.html (accessed: 20 January 2021)

Rücker, Daniel/Kugler, Tobias, New European General Data Protection Regulation, 2018

Schachtschneider, Karl A., Das Sittengesetz und die guten Sitten, in: Bernd Becker/Hans Peter Bull/Otfried Seewald (eds.), Festschrift Werner Thieme zum 70. Geburtstag, 1993, pages 195-225

Schmitt, Marion/Resch, Christoph, Von der Befugnis der Gerichte Daten zu verarbeiten, 4 (2020), pages 134-141

Schneider, Hans, Gesetzgebung – Ein Lehrbuch – , 2. Auflage [second edition] 1991

Schulze, Gerhard, Die Sünde, 2006 (reprint, 2008)

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter, DS-GVO/BDSG, 2. Auflage [2nd edition], 2020

Simitis, Spiros/Hornung Gerrit/Spiecker, Indra, Datenschutzrecht DSGVO mit BDSG, 2019

Smolensky, Kirsten Rabe, Rights of the Dead, Hofstra Law Review, vol. 37 no 3 (2009), pages 763-803

Solmecke, Christian and *Kocatepe, Sibel,* DSGV für Webseiten-Betreiber, 2. Auflage [2nd edition], 2018

Streinz, Rudolf (ed.), EUV/AEUV, 3. Auflage [3rd. editiion]. 2018

Stern, Klaus, Das Staatsrecht der Bundesrepublik Deutschland, Band [volume] I, 2. Auflage [2nd edition], 1984; volume III/1, 1988

Stern, Klaus, Der Staat des Grundgesetzes, herausgegeben von [edited by] Helmut Siekmann, 1992

Sydow, Gernot, Europäische Datenschutzgrundverordnung, 2. Auflage [2nd edition], 2018

Taeger, Jürgen/Gabel, Detlev, DSGVO – BDSG, Kommentar, 3. Auflage [3rd edition], 2019

Voigt, Paul/von dem Busche, *Axel,* The EU General Data Protection Regulation (GDPR), 2017 (reprint)

von Münch, Ingo, Kriele, Martin, Recht-Politik-Moral, in: Joachim Burmeister et alia (Hrsg.) [editors], Verfassungsstaatlichkeit, Festschrift für Klaus Stern zum 65. Geburtstag, 1997, pages 49-61

Watteler, Oliver und Ebel, Thomas, Datenschutz im Forschungsdatenmanagement, in: Uwe Jensen, Sebastian Netscher and Katrin Weller (Hrsg.) [editors], Forschungsdatenmanagement sozialwissenschaftlicher Umfragedaten, 2019, pages 57-80

Welzel, Hans, Naturrecht und materiale Gerechtigkeit, 1962

Wolff, Heinrich Amadeus/Brink, Stefan (editors.), Beck Online Kommentar Datenschutzrecht, 34. Auflage [34th edition] (2020)

11. List of Abbreviations

BDSG	*Bundesdatenschutzgesetz* [Federal Act on Data Protection]
BGH	*Bundesgerichtshof* [highest German ordinary court]
BGHZ	*Entscheidungen des Bundesgerichtshofs in Zivilsachen* [private law section of the highest German ordinary court]
BVerfG	*Bundesverfassungsgericht* [German Federal Constitutional Court]
BVerwG	*Bundesverwaltungsgericht* [German Federal Administrative Court]
BVerfGE	*Entscheidungen des Bundesverfassungsgerichts* [Collection of Judgments of the German Federal Constitutional Court]
BVerfK-K	*Bundesverfassungsgericht, Kammerentscheidung* [German Federal Constitutional Court, judgment of a Chamber of the Court]
cf.	see, for
CFR	Charter of Fundamental Rights of the European Union
CYIL	Czech Yearbook of Public & Private International Law
DPD	Data Protection Directive
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
ECR	European Court Reports
Ed(s).	Editor, editors, edition
ePrivacy Directive	Directive 2002/58/EC on privacy and electronic communications
et seq.	and following
EUWA	European Union (Withdrawal) Act 2018
GFCC	German Federal Constitutional Court [*Bundesverfassungsgericht – BVerfG*]
GDPR	General Data Protection Regulation
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HGR	Handbuch der Grundrechte
IDPR	Regulation on Data Processing by EU Institutions
ISP	Internet Service Provider
LED	Law Enforcement Directive

NJW	*Neue Juristische Wochenschrift* [New Weekly Law Review]
NVwZ	Neue Zeitschrift für Verwaltungsrecht [Law Review on Administrative Law]
OJ	Official Journal of the European Union
RG	*Reichsgericht* [Highest Court of the German Empire]
RGZ	*Entscheidungen des Reichsgerichts in Zivilsachen* [Highest Court of the German Reich in Private Law Cases]
TCA	EU-UK Trade and Cooperation Agreement
WP	Article 29 (Data Protection) Working Party

12. List of Figures

Appendix 1: Text of Most Relevant Legal Provisions

European Convention for the Protection of Human Rights and Fundamental Freedoms

Article 8

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Charter of Fundamental Rights of the European Union

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Article 51

Field of application

1. The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.

2. The Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties.

Article 52

Scope and interpretation of rights and principles

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties.

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

4. In so far as this Charter recognises fundamental rights as they result from the constitutional traditions common to the Member States, those rights shall be interpreted in harmony with those traditions.

5. The provisions of this Charter which contain principles may be implemented by legislative and executive acts taken by institutions, bodies, offices and agencies of the Union, and by acts of Member States when they are implementing Union law, in the exercise of their respective powers. They shall be judicially cognisable only in the interpretation of such acts and in the ruling on their legality.

6. Full account shall be taken of national laws and practices as specified in this Charter.

7. The explanations drawn up as a way of providing guidance in the interpretation of this Charter shall be given due regard by the courts of the Union and of the Member States.

Treaty on the Functioning of the European Union

Article 16

(ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

General Data Protection Regulation

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 4.5.2016 L 119/32 Official Journal of the European Union EN

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are

determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the 4.5.2016 L 119/33 Official Journal of the European Union EN framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14)'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) 'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the

latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51; 4.5.2016 L 119/34 Official Journal of the European Union EN

(22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1) [footnote: (1) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1)];

(26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific 4.5.2016 L 119/36 Official Journal of the European Union EN processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with para-graph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Appendix 2: GDPR: Guidelines, Recommendations, Best Practices[345]

- Guidelines 10/2020 on restrictions under Article 23 GDPR – version for public consultation
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – version for public consultation
- Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 – version for public consultation
- Guidelines 08/2020 on the targeting of social media users – version for public consultation
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR – version for public consultation
- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR – Adopted after public consultation
- Guidelines 05/2020 on consent under Regulation 2016/679
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak
- Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak
- Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies – version adopted after public consultation
- Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications – version for public consultation
- Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) – version adopted after public consultation
- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – version adopted after public consultation
- Guidelines 3/2019 on processing of personal data through video devices – Adopted after public consultation
- Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725)
- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects – version adopted after public consultation
- Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 – version adopted after public consultation

[345] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

- Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) – version adopted after public consultation
- Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation
- Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679
- Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation – version adopted after public consultation

Appendix 3: GDPR related WP29 Guidelines[346]

During its first plenary meeting the European Data Protection Board endorsed the GDPR-related WP29 Guidelines:

1. Guidelines on consent under Regulation 2016/679, WP259 rev.01
   Superseded by Guidelines 05/2020 on consent under Regulation 2016/679
2. Guidelines on transparency under Regulation 2016/679, WP260 rev.01
3. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01
4. Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01
5. Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01
6. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01
7. Guidelines on Data Protection Officers ('DPO'), WP243 rev.01
8. Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01
9. Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR
10. Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, WP 263 rev.01
11. Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264
12. Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265
13. Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01
14. Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01
15. Adequacy Referential, WP 254 rev.01
16. Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253

[346] Ibid.

Appendix 4: Example (i) of a Privacy Statement. EU Commission[347]

Privacy statement for users registered with the European Commission's Identity and Access Management Service (IAMS)

(DPR-EC-03187)

1. INTRODUCTION

The European Commission (hereafter 'the Commission') is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to processing operation 'Identity & Access Management Service (IAMS)' including EU Login, undertaken by EC DIGIT D3, is presented below.

2. WHY AND HOW DO WE PROCESS YOUR PERSONAL DATA?

Purpose of the processing operation: The European Commission's Identity & Access Management Service (IAMS) provides a common way for individuals to register or be registered for access to a number of different Commission information systems or services.

EC DIGIT D3 collects and uses your personal information to manage user populations and their rights in the context of IT systems. The main purpose is to ensure the appropriate level of security is applied in a consistent fashion across Commission IT services with the ability to identify the user of the service, authenticate that user, and / or determine his or her authorisations and roles within the context of their service. The IAMS allows not only the authentication of individual that have an employment relationship with EU Institutions (EU Staff), but also self-registered individuals can create an EU-login account worldwide.

Additional purposes for this processing operation, regarding individuals that have an employment relationship with EUIs, are the following:

- services, allowing individuals contact details to be found (e.g. e-mail address book or telephone directory)
- selection of individuals from lists, usually based on some selection criteria
- construction of lists of individuals, primarily e-mail distribution lists
- customisation of user interfaces according to users' individual characteristics

The processing is automated and performed by means of computer/machine.

[347] https://ecas.ec.europa.eu/cas/privacyStatement.html?loginRequestId=ECAS_LR-36110474-DxSxMzt9e9vJezgJ97eVDumgOms2a1jjGZqup3bqqEjIzZVY8Bek69X4zhMtSH7G5zGZDy4OIsSeHXJ9bfJq3O1-yntOf97TTHqx7OLH5zM5i4-2ANGVJfTTyTJzLUM9iNQlhJj7N89QsdmopznXNPuQbxxUAevRk6znh8H8N2p4SO4DjuhaGRLFb9zZliS4DzINNr.

Your personal data will not be used for an automated decision-making including profiling.

Individual Commission sites that rely on IAMS for commonly required personal data, may nevertheless collect additional personal data themselves. This data processing will be covered by the sites' own privacy statements.

3. ON WHAT LEGAL GROUND(S) DO WE PROCESS YOUR PERSONAL DATA

We process your personal data, because:

(a) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;

The processing is necessary for the performance and support of tasks carried out by the institution as mandated by the Treaties, in particular Articles 3, 4, 5, 6, 7, 11, 17, of the Treaty of the European Union and Articles 2, 4, 67, 310, 325 of the Treaty of the Functioning of the European Union.

Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission and Information Security Policy and Internal Rules for handling ICT Information Security Incidents, the Commission Information Systems Security Policy C(2006)3602.

Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45, 14.6.1962, p. 1385), as last amended by Commission Delegated Regulation (EU) 2016/1611 of 7 July 2016.

This processing operation is also in line with Regulation (EU) 2018/1724 on establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 and within the scope of the EC's eGovernment Action Plan 2016-2020 on accelerating the digital transformation of governments.

The above-mentioned legal basis applies to the EU-login users that have an employment relationship with the EU Institutions, agencies and Bodies (EU Staff).

The personal data of the self-registered individuals is processed based on their consent after having read, understood and agreed to this privacy statement. Consent can be withdrawn at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. WHICH PERSONAL DATA DO WE COLLECT AND FURTHER PROCESS?

In order to carry out this processing operation EC DIGIT D3 collects the following categories of personal data:

For EU Institutions staff, IAMS is processing only identification data (to identify the individuals):

- Personal information:
    - first, middle and last name(s) as provided by the HR Systems,
    - date of birth
    - personal title
    - history of changes in the name
    - an unique number per EU Institution, Agency or Body attributed by the HR System of each entity (Personal Number)
    - an unique identification number in attributed by the Commission HR System (Per_ID)

Based on the above, IAMS generates a unique:

- username or account (based on specific rules)
- e-mail address (based on specific rules)

IAMS keeps a history of:

- name changes (not to create multiple identities for the same individual)
- password changes (to enforce regular changes (passwords are irreversibly encrypted))
- last authentication and authenticated account activity (Date and time of the most recent successful and unsuccessful authentication and number of good logins and failed attempts)

This additional information is used to diagnose and resolve problems and to deal with security incidents as well as to avoid duplicated accounts. This information can help in following up any doubtful/malicious activity relating to your user account.

- Administrative data (to identify the relationship with the organization):
  - the entity where the individual is assigned
  - the job title
  - the job status
  - information related to the start and end of the contract
  - office address and phone number
  - mobile phone number (for two-factor authentication, when available into the HR System)

Based on the above and on the HR "basic entitlements policy", IAMS generates:

- access rights - information about group membership (for granting access to the intended systems)

For self-registered individuals, IAMS is processing only identification data.

- Personal information (as provided by the individual during self-registration):
  - first, middle and last name(s)
  - e-mail address
  - username
  - mobile number, when provided for two-factor authentication.

For the two-factor authentication using the EU Login mobile app, the Operating System software of the mobile device is stored as well.

Alternatively, self-registered users may choose to authenticate using their social network credentials (like Facebook, Twitter, and Google) or the eID. In this case, only the Social-media/eID identifier is required. The individual may decide to provide additional information such as:

- First, last name
- e-mail address

Please note that if you choose this option, we would recommend you also read the privacy statements/notices of the related social network, since they are also applicable.

Log files for both user categories

Each time the user logs in to a site protected by EU Login, the identifier, the site and the time will be recorded in a log file. The exact time of log-out will also be recorded for security purposes.

The provision of personal data is mandatory to meet access requirement to the European Commission IT Systems. If you do not provide your personal data, the consequence is that you will not be able to get access to the mentioned IT systems.

We have obtained your personal data either from the HR system of your EU Institution, Agency or Body for the EU Institutions staff, or directly from the data subject for the self-registered individuals.

5. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

EC DIGIT D3 only keeps your personal data for the time necessary to fulfil the purpose of collection.

Data related to the European Institutions Staff are kept for as long as the user has a relationship with the European Commission.

However, the user's identifier (userid), personnel number, first/last name, and, to prevent errors, date of birth are retained for a longer period in order to:

- allow the reuse of the identifier, if appropriate, should the person require renewed access to Commission IT resources after a long absence or for assuming his/her rights for example while in retirement,
- to determine the real global identity of a user and prevent duplication of entries.

For other EU Institutions, Agencies and Bodies, the above-mentioned data, will be limited to the information provided by each one of them according to their Human Resources policy.

Data related to self-registered individuals are kept until the user personally deletes his/her EU-Login account or requests the deletion by our Unit, with the exception of e-mail addresses that need to be kept for further user support and assistance.

History of identity changes for the European Institutions staff is kept for as long as the user is active. However, the most recent entries of this data category should be kept longer to prevent duplication of entries and ensure security.

Log files are kept for 6 months.

6. HOW DO WE PROTECT AND SAFEGUARD YOUR PERSONAL DATA?

All personal data in electronic format (databases) are stored on the servers of the European Commission. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures in place. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

7. WHO HAS ACCESS TO YOUR PERSONAL DATA AND TO WHOM IS IT DISCLOSED?

Access to your personal data is provided to the Commission staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

Personal data is not shared with other recipients, or transferred to third countries or international organisations.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

8. WHAT ARE YOUR RIGHTS AND HOW CAN YOU EXERCISE THEM?

You have specific rights as a data subject under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a) on grounds relating to your particular situation.

For self-registered individuals:

You have consented to provide your personal data to EC DIGIT D3 for the present processing operation. You can withdraw your consent at any time by notifying the Data Controller. You may also delete your account at any time. The withdrawal will not affect the lawfulness of the processing carried out before you have withdrawn the consent.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

9. CONTACT INFORMATION

- The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact:

- For EU Institutions staff, your HR department; then all modifications will be automatically reflected in IAMS;
- For self-registered individuals, directly the Data Controller, at: EU-LOGIN-EXTERNAL-SUPPORT@ec.europa.eu.

- The Data Protection Officer (DPO) of the Commission

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. WHERE TO FIND MORE DETAILED INFORMATION

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: http://ec.europa.eu/dpo-register.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-03187

Appendix 5: Example (ii) of a Privacy Statement. EU Research Infrastructure EUDAT[348]

Privacy Policy of EUDAT

This Application collects some Personal Data from its Users.

The EUDAT platform, URL: eudat.eu , (hereinafter referred to as "Site" or "Application") abides by the following principles when handling personal information:

- We collect a small amount of personal information about our users in order to provide them with our content, products and services;
- We limit the sharing or disclosure of this personal information to our needs or to comply with applicable legal requirements;
- We give users meaningful choices over the use of their personal information;
- We strive to protect the personal information that we hold.

This Privacy Notice describes the policies applied with respect to the personal information collected through the Site, or when the Site communicates with its users ("you" or "user"), and the choices that are made available to them. "Personal Information" means any information that relates to an identified or identifiable individual.

The project is co-funded by the European Commission, therefore the EU data processing law applies. The policy on "protection of individuals with regard to the processing of personal data by the Community institutions" is based on EU regulation as described https://ec.europa.eu/info/legal-notice_en#personal-data-protection

Data Controller

EUDAT CDI Ltd.

Data Controller email: info[at]eudat.eu

Data Processor

Trust-IT Srl
Via Nino Bixio, 25
56125 Pisa, Italy
P.IVA e C.F. 01870130505
info[at]trust-itservices.com

Commpla Srl
Via Nino Bixio, 25
56125 Pisa - Italy
P.IVA 01958380501
contact[at]commpla.com

1. Your consent

[348] https://eudat.eu/privacy-policy.

Your use of the Site signifies that you agree will all terms of this Privacy Notice. If you communicate with us and provide us with personal information, we will assume that you agree that we can use this information to communicate with you. If you disagree with any part of this Privacy Notice, please do not use the Site or communicate with us.

2. Scope

This Privacy Notice applies solely to personal information that the Application collects through the Site or through any electronic communications that you send to the Application, as indicated on the Site (Personal Data). It does not apply to the websites of third parties, such as business partners or sponsors, to which the Site may link. The Application does not endorse, nor is responsible for the content of these third-party websites, or their policies or practices.

If you provide any personal information to or through third party websites, your transaction will be subject to the terms and conditions and the privacy policies of these third-party websites.

3. What information we collect, and how we collect it

The Application manages different types of data, all in compliance with the current European legislation on Data Protection. Any Data concerning the User is collected to enable the Owner to provide its services, as well as for the following purposes: Tag Management, Displaying content from external platforms, Analytics, Contacting the User, Managing contacts and sending messages, Interaction with data collection platforms and other third parties.

The Personal Data used for each purpose is outlined in the specific sections of this document.

Among the types of Personal Data that this Application collects, by itself or through third parties, are: Cookies, Usage Data, first name, last name, email address, various types of Data and city.

Data voluntarily supplied by the User -- The web platform is designed to allow users to browse through it without providing any contact information. However, certain areas may require, or allow for, the submission of personal information, such as when a user fills out a newsletter form or contacts us. As an example, clients of the Application need to register to become part of the web site community and use the Application solutions.
The data collected and further processed are necessary to access the Application, as well as for communication and follow-up activities. Appropriate, detailed information is provided to the User and, where required, consent for the processing of Personal Data is obtained before a given service is activated. Said consent may be revoked at any time, whereby the ability to use the service in question ceases.

Users are responsible for any third-party Personal Data obtained, published or shared through this Application and confirm that they have the third party's consent to provide the Data to the Owner.

Cookies -- Any Cookies or other tracking tools used by this Application, or by the owners of third-party services used through this Application, serve the purpose of providing the service required by the User, in addition to any other purposes described in the present document and in the Cookie Policy, if available.

4. Interaction with social networks and external platforms

This kind of service allows you to interact with social networks, or other external platforms, directly from the pages of this application. The information acquired by the Application through this interaction is in any case subject to the User's privacy settings related to each social network. If an interaction service with social networks is installed, it is possible that, even if the Users do not use the service, the latter collect traffic data relating to the pages in which it is installed. Like button and Facebook social widgets (Facebook, Inc.)

The "Like" button and Facebook social widgets are services of interaction with the social network Facebook, provided by Facebook, Inc.
Personal Data collected: Cookies and Usage Data.

Place of processing: USA - Privacy Policy
Tweet button and Twitter social widgets (Twitter, Inc.)

The Tweet button and Twitter social widgets are services of interaction with the Twitter social network, provided by Twitter, Inc.

5. Where and How the Data is processed

Location -- The Application is provided via the web portal site, whose servers are located in Ireland, and provided by Amazon Elastic Compute Cloud (Amazon EC2). Amazon Web Services comply with the General Data Protection Regulation (GDPR) https://aws.amazon.com/blogs/security/all-aws-services-gdpr-ready/
The Data is processed at the Data Controller's operating offices and in any other places where the parties involved in the processing are located. For further information, please contact the Data Controller.

Duration of Processing -- Data processing is limited to the time necessary to perform the service requested by the User. Unless otherwise requested by the European Commission, any data kept to the purposes of a project is retained for the duration of the project, plus the period requested by the European Commission (typically 3 years) after the project end. However, the User can ask at any time to interrupt the processing of the Data or have Data cancelled.

Log information-- Our server software automatically gathers general information from all users. For example: IP address, computer type, screen resolution, OS version, domain name, location, date and time of the visit, page(s) visited, time spent on a page, website from which the user came, action taken by the user when leaving our Site. Some of this information is provided directly by the user's browser, the remainder is obtained through cookies and tracking technologies.

Registration information -- Webinars and other events may be provided with the assistance of unaffiliated third-party vendors, which may require that the vendors have access to personal information such as name, company, and email address. These vendors will provide us with this information, so that we can keep track of who registers to, or attends these events. In this case, the information that you provide as part of this registration will be subject to both our Privacy Notice and the applicable privacy statement posted on the vendor's website.

Children -- The Site is not intended for children. Nor does the Application knowingly collect personal information from children.

6. How we use this information

The Application uses personal information for the following:

- Fulfilment of requests -- We may use your personal information to deal with your inquiries, register you to our events, and send you the publications or documents that you request.
- Internal business purposes -- We may use the collected information for internal business purposes, such as for audits or to track attendance at events.
- Site operation -- We use cookies to assign a unique identifier to a user's computer.
- Statistical analysis -- We use aggregated data about Site usage (which do not identify a specific user), such as the number of users who have visited certain pages of the Site, or how long users are spending on a particular page, in order to develop statistics as to the use of the Site, so that we can understand how users interact with the Site, to improve its content, products, or services.
- Displaying content from external platforms

7. To whom your personal information is disclosed

The **Data Controller** processes the Data of Users in a proper manner and takes appropriate security measures to prevent unauthorized access, disclosure, modification, or destruction of the Data.

The **Data processing** is carried out using computers and/or IT enabled tools, following organisational procedures and practices strictly related to the purposes indicated. The Data Controller processes the Data of Users in a proper manner and shall take appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Data. In addition to the Data Controller, in some cases, the Data may be accessible to certain types of persons in charge, involved with the operation of the site (administration, sales, marketing, legal, system administration) or external parties (such as third-party technical service providers, mail carriers, hosting providers, IT companies, communications agencies) appointed, if necessary, as Data Processors by the Owner. The updated list of these parties may be requested from the Data Controller at any time.

The Application Members -- We may share personal information with members of a Consortium for the purpose of creating a knowledge base and potential customer leads for the exploitation of results and assets.

Law enforcement; compliance -- We may use or disclose personal information to any third party (a) if we believe that we are required to do so by law; (b) to comply with legal processes or respond to requests from governmental or public authorities; (c) to prevent, investigate, detect, or prosecute criminal offenses or attacks on the technical integrity of the Site or network; (d) to enforce our Terms and Conditions; or (e) to protect the rights, privacy, property, business, or safety of the Application, its business partners, employees, members, Site users, or the public. Unless prohibited by applicable law, we will inform you if a third party requests access to personal information about you.

8. Right to access and rectification

You have the right to have access to the personal information that we hold about you, and to have this information corrected and amended, as defined in the GDPR art. 12, 15, 16. To do so, please contact us as indicated in section 16. However, please be aware that in some cases, the administrative and technical burden associated with the retrieval of archived data may be substantial. We would need to be compensated for this effort in a manner that is consistent with our actual cost.

9. Right to erasure

You have the right to request that we delete any Personal Information that we hold about you. The Application is compliant with the Right to Erasure as defined in the GDPR, art. 17. If you would like us to erase the Personal Information that we hold about you, please contact us by email at **info@eudat.eu**

10. Right to object

You have the right to object at any time to the processing of your personal data, on grounds relating to your particular situation, as defined in the GDPR, art. 21. Please note that all the data you provide on this website will be used only for delivery of the services provided by the Application, as described in section 5. If you would like to apply your right to object, please contact us by email at **info@eudat.eu**.

11. Retention of information

We will retain personal information about a user for as long as necessary to fulfil the purposes outlined in this Privacy Notice, unless a longer retention period is required by law and/or regulations. The User can always request that the Data Controller suspend or remove the data.

12. Security

The Application seeks to adopt commercially reasonable security measures consistent with industry practice to protect personal information under its control against loss, misuse, and alteration. However, we cannot guarantee

the security of our servers, the means by which personal information is transmitted between your computer and our servers, or any personal information that we receive through or in connection with the Site.

We attempt to strike a reasonable balance between security and convenience. Emails are usually sent as unencrypted text. If misrouted or intercepted, an unencrypted email could be read easily. If there is a matter that requires high security or confidentiality, please keep us informed about the sensitivity of the information, and do not send the related information by email.

13. Jurisdiction

The Application does not represent or warrant that the Site is appropriate or available for use in any particular jurisdiction. Those who choose to access the Site do so on their own initiative and at their own risk, and are responsible for complying with all local laws, rules, and regulations that apply to them.

We may limit access to the Site to any person, geographic area, or jurisdiction that we choose, at our sole discretion.

14. Inquiries and Complaints

If you have any questions, comments, or complaints about this Privacy Notice, or the use, management or disclosure of personal information collected on or through our Site, please contact us at **info@eudat.eu**.

15. Updates to the Privacy Notice

We update this Privacy Notice from time to time. If the changes are significant, we will post prominent notification on this Site for a reasonable time to inform you of these changes. Unless, and until, you object in writing, by contacting us at **info@eudat.eu**, all changes will apply to the existing information about you that the Application already holds, and the personal information collected from the effective date of the revised Privacy Notice. Your use of the Site following the effective date of any revision will constitute your acceptance of the terms of the updated Privacy Notice.

16. How to Contact Us

If you have any questions, comments, or complaints, regarding this Privacy Notice, or our privacy, security or data protection practices, please contact us by email at **info@eudat.eu**.

Effective Date: May, 25, 2018 - Ver 1.2