Stiftung
Familienunternehmen

Disclosure Requirements of Family Companies

Analysis of status quo and assessment under data protection law

Publication details

Published by:

Stiftung Familienunternehmen

Stiftung Familienunternehmen
Prinzregentenstraße 50
80538 Munich
Germany

Tel.: +49 (0) 89 / 12 76 400 02
Fax: +49 (0) 89 / 12 76 400 09
E-mail: info@familienunternehmen.de
www.familienunternehmen.de

Prepared by:

Prof. Ralf P. Schenke
Julius Maximilians University Würzburg, Germany
Professor of Public Law, German, European and International Tax Law
Tel.: +49 (0) 931 / 31 82 360
Fax: +49 (0) 931 / 31 86 070
E-mail: schenke@jura.uni.wuerzburg.de
www.jura.uni-wuerzburg.de/en/chairs-and-professorships/schenke/home/

Prof. Christoph Teichmann
Julius Maximilians University Würzburg, Germany
Professor of Civil Law, German and European Commercial and Company Law
Tel.: +49 (0) 931 / 31 82 327
Fax: +49 (0) 931 / 31 82 980
E-mail: teichmann@jura.uni-wuerzburg.de
www.jura.uni-wuerzburg.de/en/chairs-and-professorships/teichmann/home/

ISBN: 978-3-942467-67-4

Quotation (full acknowledgement):

Stiftung Familienunternehmen (eds.): Disclosure requirements of family companies – Analysis of status quo and assessment under data protection law, prepared by Prof. Ralf P. Schenke and Prof. Christoph Teichmann, Munich 2018, www.familienunternehmen.de

Contents

Summary of main results

1. In today's economic world, companies are subject to countless statutory reporting requirements. These requirements are met at regular intervals by making submissions to the competent authorities, which process the information as part of their responsibilities and, in doing so, are subject to the applicable data protection law. A subset of this group of requirements is what are known as "disclosure requirements", which require disclosure erga omnes. This kind of disclosure to the general public affects the right to data privacy in a particular way because it is impossible, legally and in practice, to enforce the processing and use of data in compliance with data protection requirements, if the data is known to everyone. Legislators are therefore subject to a more stringent requirement to examine and justify their actions under data protection law when imposing disclosure requirements.

2. Disclosure requirements are by no means a novelty in the German and European legal system. Commercial and company law looks back on a long tradition of disclosure requirements of this kind. Examples include disclosure in the commercial register, the requirement to publish the annual financial statements of corporations and the disclosure requirements of the capital market. These classic disclosure requirements are justified by the fact that they contribute to the functioning of certain markets and reduce the transaction costs associated with collecting information.

3. However, the transparency register established at the end of October 2017 suggests that a paradigm shift is under way: firstly, the transparency register captures personal data of natural persons. Secondly, its primary function is not to serve market participants, but the public interest (fight against money laundering and terrorism). And thirdly, access to the register will not be limited to the competent authorities that need it to discharge their duties, but it is intended as a source of information for everyone.

4. This affects family companies in particular because, in combination with an array of different disclosure requirements, it will force them to give the public revealing insights into the asset structure and income situation of the companies and the family members associated with them. The restrictions and burdens associated with this have an enormous impact, ranging from an increased risk of becoming victims of crime to interference with a large variety of social relationships. Knowledge of an individual's wealth may lead to supposed "friends" to behave opportunistically. In the public debate, this kind of information will probably not always be used for the noble purposes intended by legislators when they introduced the transparency register. There are good reasons, therefore, why individuals have so far been allowed to decide for themselves with whom to share details of their financial situations.

5. There are signs of a similar increase in disclosure requirements in the area of tax. The European Commission is planning to make the country-by-country report, which has to date only been shared among the tax authorities of the Member States, subject to a general disclosure requirement. This report contains – on a country-by-country basis – key corporate data on profitability, lines of business and tax burden, meaning that its publication would be in conflict with the principle of tax confidentiality.

6. From a legal policy perspective, the new disclosure requirements are often justified citing "transparency" as a catchword. These kinds of demands have a long tradition in legal philosophy, which can be traced back to the age of Enlightenment. However, in the past, transparency requirements were always targeted at the state and were used to oversee and rein in state power.

7. To demand transparency and disclosure from private individuals amounts to conscious or unconscious mislabelling. The claim of transparency, which has positive connotations and is meant to make government actions open and verifiable, is turned against citizens, subjecting them to social controls that have no foundation in the rule of law. Effective control of financial power by civil society is not an accidental side effect of the disclosure requirements, but – as evidenced in the recitals to the Fifth Money Laundering Directive of 2018 – a declared objective of the legislation.

8. An antithesis to this development is the data protection debate, at the centre of which has traditionally been the basic right to data privacy. This basic right guarantees that individuals in principle have the right to decide on how their personal data can be used. It was "developed" 35 years ago in the Federal Constitutional Court's census ruling. Violations of this right are subject severe jail terms, which have been introduced to deal with what is called the intimidating effect – namely, that in many cases, the observation and storage of personal data often triggers a change in behaviour. This makes data protection a basic prerequisite of individual freedom, especially in the context of a modern information society.

9. From the perspective of data protection, company disclosure requirements have a particular quality and depth of intervention. Those forced to disclose personal data to the public lose control over its subsequent use. Data protection guarantees and assurances, such as the prohibition on changing the purpose as well as deletion and information requirements in particular, become moot in practice once the personal data is in the public domain.

10. The increase in company disclosure requirements is based on international agreements initiated by, or at the level of, the OECD. The anti-money laundering initiative is driven by the Financial Action Task Force (FATF), while the curtailment of damaging international tax competition and improvements to international tax fairness are addressed by the BEPS (base erosion and profit shifting) process. In the first step, the international agreements were implemented in directives adopted by the European Union and subsequently transposed into national law.

11. The right in principle to drive these reform agendas is probably not in dispute. What we can object to, however, is that their implementation at the level of the European Union goes beyond the international agreements, thus writing additional disclosure requirements into law without taking account of threats to civil liberties as a result of violations of data protection requirements. This applies to both the creation of the transparency register and the debate about public country-by-country reporting.

12. The tendency largely to disregard data protection requirements when imposing disclosure obligations is probably attributable to the fact that data protection considerations feature relatively rarely in discussions about commercial, company, and, to some extent, even tax law. By the same token, typical advocates of data protection rights have little interest in issues relating to company or tax law. A key aim of this study is to bring together these two important strands of legal development.

13. European data protection law has undergone turbulent changes in recent years, championed and driven by the ECJ, which has made this issue its own and set data protection standards that exceed even those of Germany's Federal Constitutional Court. To be compatible with the data protection guarantees laid down in the Charter of Fundamental Rights (Art. 7 and 8 CFREU), interventions must be limited to what is "absolutely necessary".

14. The juxtaposition of the transparency register and the planned public country-by-country reporting with recent case law of the ECJ, especially its rulings on data retention, reveals a long list of deficiencies: Firstly, there was no attempt to investigate less restrictive means of achieving the – quite legitimate – legal policy objectives. Secondly, it is against EU rules to collect data without a valid reason, i.e. without first considering, for example, whether the affected party is in any way exposed to increased money laundering risk. Thirdly, the assurances required under procedural law have not been implemented at the level of the Money Laundering Directive; to leave them to the discretion of the Member States is not compliant with data protection requirements. These kinds of assurances relate to rules on the right to information on who has retrieved the data and how it is used, as well as the right to object and demand deletion, without which it is impossible to ensure compliance with the prohibition on changing the purpose of data collection.

15. For as long as these requirements are not met, information may not be provided. In addition, data protection aspects should in future be adequately taken into account as early as the international level. This is the only way to avoid making agreements that subsequently fall foul of the data protection requirements under EU law. However, this is not currently a problem, because the disclosure requirements being investigated here are not planned or called for as part of the BEPS process or by the FATF. At the level of EU law, this should therefore make it a lot easier to resist implementing more than international agreements require, and either to abandon the imposition of disclosure requirements altogether, or to scale them back to a level that is compatible with the requirements of European data protection law.

A. Introduction to the issues

I. Disclosure requirements as a subset of company reporting requirements

These days, business activities entail a multitude of disclosure and reporting requirements. They are based on a variety of laws and pursue different objectives, affecting almost all areas of law. Prominent examples of company reporting requirements include, among others, the requirement to file tax returns (section 149 of the AO) or the reporting requirements under social security law (section 28a of the SGB-IV). In addition, almost any economic activity is subject to specific approval and reporting requirements, for example in notification and approval proceedings under construction, environmental and trade law (e.g. article 64 (1), (2) of the BayBO, section 10 (1), (2) of the BImSchG, section 14 (1) of the GewO).

In the cases mentioned above, the information is submitted to the designated authority that has legal competence. These reporting requirements represent a considerable bureaucratic burden for the companies concerned. The legally imposed reporting requirements are not always coordinated in such a way that duplication is avoided. These kinds of administrative burdens weigh particularly heavily on family companies, which are often small or medium-sized.

In recent times, however, these legal reporting requirements have reached a new dimension. Legal policies are making increasing demands on companies to provide information that is subsequently made available to the public. This "publicity" in the actual sense of the word, through which information is made accessible to the general public,[1] is very distinct from the reporting requirements mentioned earlier: the latter merely entails information being collected by an authority or other public body, which is invariably subject to the rule of law and democratic oversight. What is more, confidential treatment of the information is largely guaranteed purely by the facts of the matter, because only a limited number of individuals gain access, and the individuals concerned are normally trained in such a way that they can be expected to process the data correctly.

The circumstances are very different in the case of publicity in the original sense, which leads to the dissemination of information among the general public. These kinds of disclosure requirements represent what is conceivably the most serious intervention in the right to data privacy, because published or generally accessible information can in fact be used for any purpose, and in practice this denies the holders of the basic rights the option to control how it will be used in future. Where the data allows conclusions to be drawn about business policies, there is a risk of serious economic disadvantages if competitors are in a

1 One representative example of information on how the term was coined is Jutzi, *Unternehmenspublizität*, 2017, p. 24.

position to use the published data.[2] This applies in particular if the effect of the disclosure requirements is one-sided, i.e. if only certain companies in a group of competitors are required to make disclosures.

In terms of quantity, these kinds of disclosure requirements only account for a relatively small portion of a company's overall reporting requirements, but in terms of quality, they are of particular significance, due to modern ways of processing data. Where in the past disclosures were required to maintain a register of commercial records (sections 8 ff. of the HGB) and to ensure the publication of annual financial statements (sections 325 ff. of the HGB), the trend towards the "transparent company" may have reached a whole new dimension. A prime example is the recent introduction of the transparency register (sections 18 ff. of the GwG) intended primarily to help combat money laundering.

If European lawmakers have their way, anyone will in future be able to look up information on the "beneficial owners" of a commercial enterprise in an electronic database, without having to meet any particular access requirements. This seems to indicate a paradigm shift from disclosure of company-related data intended for the market participants towards the generally accessible publication of personal data. The implications this development brings about for data protection law have so far not been studied to any exhaustive extent. The purpose of this study is to provide food for thought on this issue and, in particular, encourage a reasonable balance to be struck between the legal policy objectives pursued by lawmakers – which are quite legitimate and understandable when analysed individually – on the one hand and the protection mechanisms required under data protection law on the other.

II. The traditional concept: information for market participants

The extent of disclosures required to be published by companies has traditionally been based on the legal form under which they operate in the market. The requirements have traditionally increased along the lines of personal liability/limitation of liability and proximity to/distance from the capital market. For example, a sole proprietor or a partnership in which at least one natural person has unlimited liability is allowed to withhold some information, while – at the opposite end of the scale – a listed stock corporation regularly has to publish comprehensive information on its business activities and many other facts and circumstances related to them.

The "fundamental publicity"[3] requirements to which all commercial enterprises are subject are based on two pillars: company name law (sections 17 ff. of the HGB) and the commercial register (sections 8 ff. of the HGB). Legal forms with limited liability must additionally publish financial statements (section 325 of the HGB). Although sections 238 ff. of the HGB also require commercial partnerships to prepare financial statements, they have to publish this information only if no natural person has assumed

2 Conseil constitutionnel of 8 Dec. 2016, 2016-741 DC marginal note 103.

3 Based on Jutzi (fn. 1) p. 125.

unlimited liability (see section 264a of the HGB, which covers in particular entities with the legal form of "GmbH & Co. KG"). The publication requirements are particularly extensive for companies using the capital market. It is not without reason that listed companies are at the centre of any legal and economic analysis of disclosure requirements.[4]

Based on a conventional reading, the different levels of transparency requirements between listed corporations, corporations that are not publicly traded as well as other merchants and commercial enterprises are determined by the sensitivity of their legal transactions. Entities wanting to benefit from the trust of investors and creditors have to be prepared to grant a certain insights into the financial situation of their company.[5] In his ground-breaking post-doctoral thesis (*Unternehmenspublizität*), which was published in 2001, Hanno Merkt summarises this principle clearly: Legally enforced disclosure should be seen as the correlate of market participation.[6]

As a result, the information that has to be published in a specific case is normally based on the information needs of market participants: the business partners of a commercial enterprise need information on the liability and agency arrangements (company name and commercial register); creditors of a limited liability company need information on the company's assets available as liable capital (financial statements); investors in the capital market need information that allows them to measure financial instruments they wish to buy or sell (requirement to publish a prospectus, ad hoc disclosure requirements, other capital market information requirements).

III. The data protection dimension

To date, legal literature has predominantly discussed company-related disclosures as part of the system internal to commercial, company and capital market law. The data protection aspects of differentiating between the different owners of companies hardly play a role there,[7] so it is not surprising that there is some catching up to do. Despite some stand-alone legal precursors[8] and the Data Protection Convention

4 See Jutzi (fn. 1), p. 69 ff.

5 See e.g. OLG Cologne, decision of 8 March 1991, 2 Wx 1/91, GmbHR 1991, 423 (424).

6 Merkt, *Unternehmenspublizität*, 2001, p. 108.

7 As far as can be ascertained, Merkt's monograph, *Unternehmenspublizität*, 2001, does not address this aspect. Jutzi's *Unternehmenspublizität*, 2017, which runs to almost 700 pages, only devotes half a page to data protection (p. 676 f., marginal note 1182). The contributions to an anthology edited by Schön, *Rechnungslegung und Wettbewerbsschutz im deutschen und europäischen Recht*, 2009, demonstrate an awareness of the problem. Judgements handed down by the civil courts only contain very sporadic and tentative pointers in this direction. See e.g. OLG Cologne, decision of 8 March 1991, 2 Wx 1/91, GmbHR 1991, 423 f.; BGH, judgement of 8 February 1994, VI ZR 286/93, AG 1994, 222 ff.

8 The Hessian Data Protection Act (Hessisches Datenschutzgesetz) of 12 October 1970 is regarded as the world's first data protection law (Official Journal of the State of Hesse (Hessisches GVBl.) I 625).

of the Council of Europe[9] entered into as early as 1981, it was the census ruling handed down in December 1983 that marked the birth of modern data protection[10]. In contrast, the debate about the meaning and purpose of company disclosure requirements to protect legal transactions goes back a lot further. For disclosures relating to establishment and financial statements required under stock corporation law, it can be traced back to the 19th century.[11]

The downside of disclosure requirements is that they also give insights into the income and assets of shareholders. From a data protection perspective, it is self-evident that any obligation to share such insights with the general public should only be possible if properly motivated. In an economic order that ties the appropriation of scarce goods and services to the use of financial resources, an individual's income and asset situation is highly sensitive information. Its knowledge permits conclusions about the social origin, lifestyle and social status of the individuals concerned.

An obligation to disclose income and assets may impair the spontaneous nature of social interaction in a multitude of ways. Just think of a young person who has inherited a valuable interest in a company: he or she will find it difficult to distinguish between true friends and those trying to take advantage. In addition to economic consequences, such as competitive disadvantages, the impact of unfettered publicity on an individual's social life ranges from class envy to legitimate concerns that social relationships are entered into only for strategic reasons, because third parties hope to derive financial benefits from a friendship or even a more intimate relationship. What is more, as income and assets rise, so does the risk of falling victim to criminal activities.[12]

As a starting point, therefore, there are valid reasons for allowing individuals to decide whether and to what extent they want to grant others insights into their income and asset situations. The requirement to disclose personal information is an exception for which valid reasons must be provided. During the general debate on disclosure requirements, this data protection requirement is at risk of receding into the background.

IV. Is the transparency register spearheading a general paradigm shift?

At present, there seems to be a particularly urgent need to emphasise the data protection perspective, because the introduction of the transparency register, which is governed by sections 18 ff. of the GwG,

9 Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Federal Law Gazette (Bundesgesetzblatt, BGBl.) 1985 II p. 539).

10 Rulings of the Federal Constitutional Court (Entscheidungen des Bundesverfassungsgerichts, BVerfGE) 65, 1 ff.

11 Many examples represented here by Merkt (fn. 6), p. 51 ff. and Jutzi (fn. 1), p. 422 ff.

12 G. Kirchhof, "Transparenzregisterdaten für jedermann?", ZRP 2017, 127.

which is in turn based on the Act Implementing the Fourth Money Laundering Directive[13], indicates a true paradigm shift: This register imposes disclosure requirements based on economic activity that has only a very loose association with market participation. The primary objective is not to inform market participants, but to prevent and investigate crimes (in particular money laundering, terrorism financing and tax evasion).

The data to be entered in the transparency register includes first and last name, date of birth, place of residence and the nature and extent of the economic interest of certain beneficial owners of organisations (section 19 (1) of the GwG). Organisations include not only corporations, but also partnerships, with the exception of civil law partnerships (section 20 (1) of the GwG). Included are both the legal form of the German limited liability company (GmbH), which is very common among small and medium-sized enterprises, and those of partnerships such as the OHG (section 123 of the HGB) and partnerships limited by shares (section 161 of the HGB), which are registered partnerships within the meaning of section 20 (1) sentence 1 of the GwG; the latter are particularly relevant for family companies. In each case, the beneficial owners must be registered. They are defined as natural persons who directly or indirectly hold more than 25 per cent of an organisation (section 3 (1) and (2) of the GwG).

Unlike the commercial register, which can be accessed by anyone (section 9 (1) of the HGB), there is currently no open access to the transparency register. Except for the authorities and other parties authorised and obligated by section 23 (1) nos. 1 and 2 of the GwG, any party wishing to access the information will have to have a legitimate interest in doing so and provide evidence of such interest to the office keeping the register (section 23 (1) no. 3 of the GwG). As evidenced in the explanatory memorandum, this kind of interest is to be attributed to non-governmental organisations (NGOs) working against money laundering, its predicate offences and terrorism financing, as well as specialised journalists conducting research in this area.[14] Since this kind of access hurdle is low and will be difficult to control, it is to be expected that data previously treated with utmost sensitivity will get into the public domain without the consent of the individuals affected. This concern is reinforced by the latest reform of the Money Laundering Directive, which plans to give everyone free access to the transparency register (see C.II.1.g for details).

The introduction of the transparency register hints at a shift in balance between the information interests of authorities and the public on the one hand and the protection of the right to data privacy of the affected individuals on the other, and this is exacerbated by similar developments in other areas of the law. This trend is particularly noticeable in the area of tax law. Up to now, tax confidentiality (section 30 of the AO) has been a trade-off for the far-reaching disclosure requirements and duties to cooperate.[15]

---

13 Act Implementing the Fourth EU Money Laundering Directive, Interpreting the EU Funds Transfer Regulation and Reorganising the Financial Intelligence Unit of 23 June 2017 (BGBl. I p. 1822).

14 Bundestag publication (Bundestagsdrucksache, BT-Drs.) 18/11555, p 133.

15 BVerfGE 67, 100 (139); 84, 239 (280); BVerfG, DStRE 2004, 396 (400).

When officials are required to keep tax information confidential (section 30 (1) of the AO), taxpayers have the assurance that the tax authorities will not use the extensive information they hold for other, non-tax purposes. However, tax confidentiality serves not only the private interests of taxpayers by keeping their tax affairs secret, but also the public interest by ensuring fair and comprehensive taxation. By strengthening citizens' trust in the administration's ability to maintain confidentiality and ensure fair treatment in the light of the extensive disclosure requirements, tax confidentiality encourages taxpayers to make full and truthful disclosures.[16]

Yet tax confidentiality has also recently been undermined in a number of ways.[17] Of great importance in this context is the international exchange of information on tax matters, which has been expanded significantly and placed on a completely new normative basis in the past few years.[18] In particular, country-by-country reporting (CbCR), which has been laid down in section 138a of the AO, has drawn a lot of attention. It requires domestic group companies, irrespective of whether they are domestic parent companies or domestic subsidiaries of foreign parent companies, to prepare a group report on a country-by-country basis and submit it to the Federal Central Tax Office. The reporting requirement applies only to international groups whose revenue exceeds a threshold of €750 million. The European Commission intends to make the country-by-country reports accessible to the public in future and has launched a legislative initiative to this effect. This would mean a fundamental change to the nature of the reporting requirements, replacing tax confidentiality with a principle of tax publicity.

V. Need for a holistic view

The more stringent disclosure requirements outlined above and the inevitable downside of concessions on the right to data privacy pursue different objectives and have been the subject of heated discussions in legal policy circles.[19] It is clear, however, that this stand-alone analysis of individual disclosure requirements misses the mark, as it fails to consider that the intense nature of the impact on those affected may only arise from the combined effect of stand-alone measures. Repeated references to the

16 Alber, in: Hepp/Spitaler, section 30 of the AO marginal note 7.

17 Instructive summary of the exemptions from tax confidentiality provided by Rüsken, in: Klein, *Abgabenordnung*, 13th ed. 2016, section 30 marginal note 110.

18 See detailed information in C.III.2.c) below (p. 58).

19 Examples relating to the transparency register include: Kotzenberg/Lorenz, "Das Transparenzregister kommt", NJW 2017, 2433 ff.; Müller, "Das Geldwäscheregister nach Art. 30 und 31 der Vierten Geldwäscherichtlinie und seine Vereinbarkeit mit der Rechtsprechung des EuGH zur Vorratsdatenspeicherung", ZStW 2016, 1021 ff.; Schaub, "Das neue Transparenzregister naht – Überblick über die Regelungen und praktische Auswirkungen für Personenvereinigungen", DStR 2017, 1438 ff.; Meinzer, "Transparenzregisterdaten für jedermann?", ZRP 2017, 127; G. Kirchhof (fn. 12); relating to the legitimacy of public country-by-country reporting: Wöhrer, "Öffentliches Country-by-Country-Reporting verfassungswidrig", SWI 2017, 25 ff.; Wakounig, in: Lang/Haunold, *Transparenz und Informationsaustausch*, 2017, p. 29; Petruzzi/Navisotschnigg, in: Lang/Haunold, *Transparenz und Informationsaustausch*, 2017, p. 51.

constitutional problems and the potential risks posed by a combination of interventions in basic rights have been made in judgements on data protection matters handed down by the Federal Constitutional Court, most recently in its BKAG ruling.[20] This means that constitutional and legal policy assessments and any analysis from an EU law perspective must take account of potential interactions between the different disclosure requirements.

A holistic view is thus also advisable because disclosure requirements are often introduced in areas of the law where awareness levels of data protection requirements are still quite low. This lack of awareness has a very real impact on the players involved: The individuals negotiating the details of the Accounting or Money Laundering Directive on behalf of the Federal Republic of Germany at the European level are not necessarily experts in data protection law. The same may apply to judges at civil courts, who in a roundabout way – for example through an action for injunctive relief – are faced with questions about the extent to which information should be disclosed, who has a right to such information and for what purpose it may be used.

VI. Objectives and methods used in the study

One of the main objectives of this study is therefore to collate and systematise the different disclosure requirements for companies and shareholders. This will provide a basis for assessing them, using higher constitutional and EU law as a benchmark, and for identifying possible conclusions for legal policy in a third step.

Data protection considerations are an additional reason for examining the existing disclosure requirements from a constitutional and EU law perspective. The downside of increased disclosure requirements is that concessions have to be made on the rights to data privacy, which are protected by Germany's Basic Law (article 2 (1) of the GG in conjunction with article 1 (1) of the GG) as well as by the Charter of Fundamental Rights of the European Union. Art. 7 CFREU guarantees respect for private and family life and Art. 8 CFREU the protection of personal data.

The weighting given to data protection is significant. Since the census ruling of 1983, the Federal Constitutional Court has handed down a large number of subsequent rulings, which create a detailed system of how the right to data privacy is to be balanced against competing public interest considerations.[21] Depending on the relevance of the personal data, the collection of information may already be prohibited in its entirety or, at the very least, the principle of proportionality has to be applied and its impact has to be cushioned, in particular by implementing organisational and procedural safeguards.

---

20 BVerfGE 141, 220 marginal notes 130; 109, 279 (323); 112, 304 (319); 130, 1 (24).

21 Many possible examples, represented here by Di Fabio, in: Maunz/Dürig, *Grundgesetz*, 2013, article 2 (1), marginal note. 177 ff.

Following some reluctance in its rulings on European data protection law, the ECJ has recently embraced the issue with greater fervour.[22] In a number of rulings handed down since 2010, it has tended to apply even stricter benchmarks than the Federal Constitutional Court. Examples of recent case law to be mindful of in this context include the Google judgement[23] as well as the second and third rulings on data retention[24]. Recent developments in European secondary law have given data protection another significant boost. 25 May 2018, the date on which the General Data Protection Regulation[25] entered into force, is an important milestone in this regard.

Answers on to how to balance the opposing interests of disclosure requirements and the protection of privacy have largely been set out by court rulings. This is a consequence of the open wording used in the normative texts, which leave ample room for different interpretations at the level of the Basic Law, the Charter, as well as of secondary law.[26] This room for manoeuvre is restricted by precedent cases which, depending on the path taken, take guidance from existing lines of case law, either confirming it or making corrections to parts of it.[27] Although the debate in the legal sciences follows its own logic of judicial rationality, it does not take place in a vacuum. Especially where enhancements to the legal system have their basis in case law, the legal discourse functions as both mirror and focal point of major social debates.[28]

This is why the legal debate on the purpose and limits of company disclosure will be be placed in a wider context as part of this study. This process will show how calls for increased company disclosure relate to the current social debate. It would, for example, be very hard to grasp the recently observed expansion of disclosure requirements in any meaningful way without the public's indignation at current irregularities

---

22 See instructive article by former ECJ President Vassilios Skouris, "Leitlinien der Rechtsprechung des EuGHs zum Datenschutz", NVwZ 2016, 1359 ff.; information on the early days of this development: Britz, "Europäisierung des grundrechtlichen Datenschutzes?", EuGRZ 2009, 1 ff.

23 ECJ, judgement of 13 May 2014, C-131/12 (Google), ECLI:EU:C:2014:317.

24 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238; ECJ, judgement of 21 December 2016, C-203/15 (data retention III), ECLI:EU:C:2016:970.

25 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 EU L 119/1 of 4 May 2016.

26 For information on the important role played by the ECJ in expanding on the GDPR, see Kühling/Martini, "Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?", EuZW 2016, 448 (449).

27 For more on the theory of path dependence and its adaptation to legal science, see Scholz, *'Einheit der Gesellschaft' versus 'Vielheit der Gesellschafter'*, 2015, p. 101 ff.

28 Representative examples of information on the interaction between socio-political and social development and between discourses and the law are Kaiser, *Die Kommunikation der Verwaltung*, 2009, p. 53 f. and Würtenberger, *Zeitgeist und Recht*, 2nd ed. 1991.

(just think of the "Panama Papers"). The legal discourse will have to bring this aspect to account, while advocating a reasoned balance between opposing public and individual interests.

Following this introduction (part A), this study breaks down into four parts: The first part contains an analysis of the interaction between increased company disclosure and central social and legal meta-discourses (part B). By placing these aspects into context, we create a basic understanding on which the subsequent assessment of the existing disclosure requirements will be based (part C). This is followed by an evaluation at the constitutional and EU levels as well as from a legal policy perspective (part D). Finally, we discuss possible conclusions for legal policy (part E).

B. Company disclosure requirements at the interface between socio-political and legal meta-discourses

Company disclosures are not a new issue. They have to date primarily been driven by economic motives, and above all the protection of creditors and investors (see I.). Recently, however, company disclosures have also found themselves at the interface with other, sometimes opposing discourses. First and foremost in this regard is the transparency debate. Transparency was recently, and especially in the Obama era, elevated to a key guideline and political demand[29] and continues to enjoy almost exclusively positive connotations (see II.). This applies to the data protection debate in a similar way. Here, too, there is a trend toward steady expansion, with the result that enhancements to data protection standards are seen as progress, while any scaling back is regarded a social step backwards (see III.). A third socio-political issue that is closely related to company disclosure requirements is the debate around tax redistribution and fairness. Helped along by a number of tax scandals, it has been lifted from a national to an international context, where it has found broad-based socio-political support (see IV.). Finally, we want to look at how the different levels of debate relate to each other (see V.).

I. Traditional economic justification for company-related disclosures

The debate around disclosure requirements from a company law perspective has traditionally been a particularly strong feature of accounting and capital markets law. Although there is an understanding in this context that disclosure requirements need to have a legitimate basis, this is mainly driven by economic efficiency considerations.[30] The ability of certain markets to function is at the centre of such deliberations. It is only fair that people who participate in the market and, in the process, use certain legal conditions to their advantage also have to accept the associated obligations. The key issues in this debate are creditor protection (accounting law) on the one hand and investor protection (capital markets law) on the other.

The key deliberations that can justify the imposition of disclosure requirements are clearly illustrated in the explanatory memorandum to the German Public Disclosure Act, which entered into force in 1969:[31] In the case of sole traders and partnerships outside of the scope of sections 264 ff. of the HGB, creditors have recourse to at least one natural person with unlimited liability. Corporations, by contrast, are only liable up to the amount of their corporate assets, thus increasing the creditors' exposure to default on receivables from the corporation. The increased transparency and disclosure requirements are therefore compensation for the heightened liability risk or, from the company's perspective, the price it has to

29 Memorandum of 21 January 2009: Transparency and Open Government (https://www.gpo.gov/fdsys/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-other-id196.pdf).

30 In detail: Jutzi (fn. 1), p. 68 ff. and Merkt (fn. 6), p. 189 ff.

31 See e.g. BT-Drs. 5/3197, p. 13.

pay for being allowed by company law to limit its liability. In addition, company-related information helps shareholders and capital market investors with their investment decisions. From a broad-based perspective, legal disclosure requirements – providing they relate to specific legal forms – strengthen the general trust in the legal forms of Aktiengesellschaft (German stock corporation) and other legal persons.[32] This indirectly also benefits those who make use of this type of legal form.

Developments in European accounting law are heading in the same direction. According to the recitals to the Disclosure Directive of 1968[33], the disclosure requirements laid down there for stock corporations, partnerships limited by shares and limited liability companies are justified with reference to the interests of creditors, who only have recourse to the company's assets to satisfy their claims.[34] In addition, European accounting law looks out for investor interests. Indirect insights are provided by the Framework of the International Financial Reporting Standards (IFRSs).[35] The Framework specifies that financial reporting should primarily meet the information needs of investors (Framework no. 10). Although the Framework also specifies other users of financial statements, such as employees, lenders, suppliers and other trade creditors, customers, governments and their agencies and, lastly, the public (Framework no. 9), the focus is on the information needs of investors, who provide risk capital to the company, and the IFRSs consciously accept that the financial statements cannot meet all the information needs of other users.

II. The transparency debate

In the area of legal policies, calls for greater transparency have in recent years come from virtually all quarters,[36] with Barack Obama's commitment "to creating an unprecedented level of openness in Government" probably marking the high point.[37] Meanwhile, transparency is today demanded not only from governmental organisations and decision processes, but increasingly also from private sector institutions. In this process, transparency, i.e. the disclosure of information, is used as a key building

32 See BT-Drs. 5/3197, p. 13.

33 First Council Directive of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community (68/151/EEC), OJ no. L 65/8 of 14 March 1968.

34 Recitals to Directive 68/151/EWG (fn. 33 above), L 65/8; also see BGH, judgement of 8 February 1994, VI ZR 286/93, NJW 1994, 1281, marginal note 25: "the legislator [aims to ensure] the protection of third parties that have, or want to establish, relations with the company concerned."

35 Even if the Conceptual Framework has not undergone the endorsement process, there are many reasons to consult it for guidance to the interpretation and application of the standards that are binding. See e.g. Merkt, "Das IFRS Conceptual Framework aus regelungsmethodischer Sicht", ZfbF 2014, 477 (490).

36 Examples from the almost unmanageable wealth of literature: C. Hood/D. Heald (eds.), *Transparency*, 2006; Jansen/Schröter/Stehr, *Transparenz*, 2010.

37 See https://en.wikisource.org/wiki/Transparency_and_Open_Government.

block in a large number of multifaceted reform agendas aimed at overcoming very divergent social, economic and political irregularities.

There are unmissable signs of a creeping, but at the same time highly problematic, shift of emphasis in the transparency debate. The original purpose of transparency was to use it as a means to control and rein in government power. Immanuel Kant put this thought succinctly in his philosophical sketch "Perpetual Peace", in which he puts together a transcendental formula of public law:

> "All actions relating to the right of other men are unjust if their maxim is not consistent with publicity."[38]

Publicity in this context is the antidote to the arcane state,[39] which has to avoid the public gaze. The concept is reflected in a large number of provisions of Germany's Basic Law, such as the guarantee of freedom of information, the strong emphasis on press freedom, the rights of commissions of inquiry and other manifestations of the democratic principle and the rule of law. These are aimed at subjecting government and the administration to public oversight and thus allowing them to be interrogated as part of the public debate.

More recently, this strand of legitimacy, which justifies transparency on the basis of democracy and the rule of law, has been joined by another aspect. Information is not only a prerequisite for oversight in a democracy and under the rule of law, it is also considered to be an economic asset. Open access to public records is then aimed at making government information freely accessible in order to open up new fields of engagement for private economic operators in a knowledge and innovation society.[40] This concept was implemented at the federal level in 2005, when the German Freedom of Information Act (Informationsfreiheitsgesetz, IFG) entered into force. Section 1 (1) of this act sets out the underlying principle of open access to public records. With the exception of Bavaria, Lower Saxony and Saxony, similar laws have also been enacted at German state level. The transmission of information must, of course, be prohibited where it impinges on the interests and rights of third parties. For this reason, section 6 sentence 1 of the IFG rules out any entitlement to access to information where such access compromises the protection of intellectual property. What is more, access to business or trade secrets may only be granted with the data subject's consent.

---

38 Kant, *Gesammelte Werke* (Collected Works), vol. 11, p. 245.

39 The term is derived from the Latin word arcanum (= secret); it refers to the "secretive state", as described by e.g. Carl Schmitt (Schmitt, *Die Diktatur*, 8th ed. 2015, p. 14 ff.).

40 Schoch, *Informationsfreiheitsgesetz*, 2nd ed. 2016, marginal note 13 f.

Much as both of the above strands of legitimacy of the transparency postulate are plausible, its most recent development is highly questionable: transparency is now demanded not only from government agents, but also from private individuals. Probably the best example in this context is the transparency register (sections 18 ff. of the GwG), which European and national legislators are hoping will contribute to combating money laundering and terrorism financing.[41] In this recent expansion, transparency is again seen as a means of oversight. However, the direction of thrust of transparency has, consciously or unconsciously, been reversed: while the traditional interpretation aimed to rein in and supervise government power, transparency is now turning into a social control tool for private individuals. From being a way to safeguard freedom and keep government in check, transparency has transformed into a tool that may be a threat to freedom. Subjecting private individuals to the scrutiny of an undefined public results in the privatisation of social control and consciously or unconsciously imposes on those affected the burden of having to justify decisions that they could previously take at their own free discretion.

This ambivalence of the transparency concept has been recognised and discussed in recent philosophical debates. One example in this regard is the monograph entitled "Die Transparenzgesellschaft" by the Karlsruhe-based social philosopher Byung-Chul Han. Published in 2012, this provocative essay unmasks the "exposure and control society" as the downside of all-encompassing transparency.[42]

III. The data protection debate

The above-described expansion of the scope of the transparency postulate to include private players is matched virtually simultaneously by the rapid advances of the data protection debate. The basic right to data protection, as developed in the famous census ruling handed down at the end of 1983,[43] is one of the most significant innovations of basic rights. The right to data privacy is an aspect of the right of personality, which is closely related to the protection of human dignity and has been laid down by the Federal Constitutional Court in article 2 (1) of the GG in conjunction with article 1 (1) of the GG.

According to the Federal Constitutional Court's classic wording of the census ruling, it guarantees the individual's right to determine independently whether to disclose personal data and how it is to be used.[44] Early on, however, data protection was elevated from a purely national to a European level. The most important milestones along the way include the European Data Protection Convention,[45] agreed at

41 Explanatory memorandum to government draft of the Act Implementing the Fourth EU Money Laundering Directive, BT-Drs. 18/11555, p. 89.

42 Han, *Transparenzgesellschaft* (Transparent society), 2012, pp. 69 ff., 74 ff.

43 BVerfGE 65, 1 ff.

44 BVerfGE 65, 1 (42).

45 BGBl. II 1981, 539.

the beginning of 1981 and thus even before the census ruling, the Data Protection Directive (Directive 95/46/EC),[46] of 1995, the incorporation of data protection in the Charter of Fundamental Rights (Art. 7, 8 CFREU) and, most recently, the General Data Protection Regulation, which entered into force in 2018.[47]

Guaranteeing effective data protection in a networked information society comes at a high cost. Nevertheless, the raising of standards in data protection law – despite the predominantly care-free behaviour of individual users – enjoys broad social acceptance.[48] When personal data is processed, this poses considerable risks to the rights and freedoms of natural persons. The potential threats range from discrimination to the risk of identity theft and fraud, financial loss and reputational damage and interference with the political opinion-forming process.[49] Criticism of the General Data Protection Regulation has therefore been levelled less at its basic approach than at alleged gaps in its cover and too much flexibility given to national governments in implementing it.

IV. The (tax) redistribution and fairness debate

An important aspect of calls for increased company disclosure is the (tax) redistribution and fairness debate.[50] Demands for limited tax publicity made in this context have received a boost, especially as a result of the recent tax scandals.[51] The antithesis or bogeyman on which this has been pinned is the tax strategy of major US companies, which, despite generating large amounts of revenue in the European Union, have paid tax only on a very small portion of their corporate profits in Europe. The OECD has used this to justify its BEPS initiative,[52] which is in turn manifests itself not only in the ATA Directive,[53] but also the requirement to prepare country-by-country reports.

---

46 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 (Official Journal of the European Communities No L 281/31).

47 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 EU L 119/1 of 4 May 2016.

48 For more on this privacy paradox e.g.: Kühling/Martini (fn. 26) (450); on criticism "of the by now deeply entrenched belief" in the expediency of data protection: Veil, "Die Datenschutz-Grundverordnung: des Kaisers neue Kleider", NVwZ 2018, 686.

49 See recital no. 75 to the GDPR (fn. 47).

50 See e.g. Weber-Grellet, "Steuerrecht und Demokratie", ZRP 2014, 82 (83).

51 Meinzer (fn. 19).

52 OECD, *Action Plan on Base Erosion and Profit Shifting*, 2014.

53 Council Directive (EU) 2016/1164 of 12 July 2016 laying down rules against tax avoidance practices that directly affect the functioning of the internal market (OJ EU L 193/1 of 19 July 2016) – known as Anti Tax Avoidance (ATA) Directive.

The revelations fuelled by the Panama Papers added to the latent simmering resentment of wealthy individuals who are known or alleged to evade their tax obligations. Even the latest reform of the EU Money Laundering Directive, which is intended to give the general public access to the transparency register, was initially justified on the basis that it is a measure to counter tax evasion (see C.II.1.g below). The EU's Data Protection Supervisor rightly criticised these plans as a problematic conflation of regulatory objectives,[54] because the Money Laundering Directive is not necessarily the appropriate regulatory vehicle for tax evasion issues. Although the reference to tax evasion was removed from the recitals in the text ultimately approved, the substance of the legal text has remained unchanged.

V. Lines of conflict and mutually reinforcing discourse levels

The above summary has shown how company disclosure requirements are increasingly moving away from being justified by citing traditional economic reasons towards being discussed from completely new perspectives and and with changed parameters. The relationship of old and new types of discourse cannot be reduced to a simple formula. Some of the demands arising from them are moving in the same direction, while others are pulling in opposite directions.

The transparency and (tax) redistribution and fairness debates argue in favour of increased company disclosure requirements, thus feeding into and reinforcing each other. For example, as is stated in the recitals to the amended Directive on Administrative Cooperation, the introduction of country-by-country reporting (CbCR) is intended to lead to greater transparency vis-à-vis the tax authorities and thus create an incentive for multinational groups to abandon certain practices and to pay their fair share of the tax burden in the countries in which they generate their profits. Increased transparency for multinational groups is therefore regarded as a key element in the fight against base erosion and profit shifting.[55] This link is likewise apparent in the amendments to the Money Laundering Directive, which will require Member States to further increase access to the transparency register. Transparency is intended to ensure that criminals can be identified who would otherwise be able to hide their identities behind complex company structures.[56]

The data protection debate, which runs counter to these trends, is not always able to withstand the pressures they exert, despite the fact that the inevitable downside of greater disclosure requirements is always concessions on data protection. The moment personal data is made public, the holder of the

54 Data Protection Supervisor, Opinion (see fn. 200 below), p. 7.

55 Recital 4 to Council Directive (EU) 2016/881 of 25 May 2016 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation.

56 Recital 14 to Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

corresponding basic rights loses control of that data. Once released, data can be freely combined with other data and, when analysed together, provide deep insights into an individual's personal circumstances. An added problem is that traditional systems for limiting the extent of intrusion are ineffective. As soon as data has been made public, it can be reproduced at will by other public as well as private parties. Although subsequent deletion or correction is feasible, in practice it becomes impossible to enforce after publication.

There is no protection from changes in the purpose of using collected data, either. A particularly salient example is tax publicity that grants general access to tax data, as is being planned in Finland, where it has already become the subject of a critical review by both the ECJ and the ECtHR (seen D.IV.1.b below).[57] The disclosure of personal tax data may well reduce the risk of tax avoidance and thus contribute to guaranteeing tax fairness and equal law enforcement. But the data can just as easily be used to satisfy personal curiosity, damage an individual's reputation in public, or identify potentially lucrative targets for criminal activities – which may in some circumstances even be a threat to the existence of the person concerned.

Increased disclosure requirements are thus inevitably linked to concessions on data protection. This is reflected in the different legal acts aimed at increasing company-related disclosure requirements: good intentions to keep data protection law in mind are not always matched by the necessary actions. As stated in the recitals, the amended Directive on Administrative Cooperation is not meant to lead to the disclosure of a commercial, industrial or professional secret or of a commercial process, and the Directive is intended to be consistent with the fundamental rights and principles, especially those recognised in the Charter of Fundamental Rights[58]. To make sure this happens, the exchange of information is subject to the provisions of the Data Protection Directive (Directive 95/46/EC) (Art. 25 of Directive 2011/16/EU)[59], which has now been superseded by the General Data Protection Regulation (GDPR).[60] This applies to the transparency register in a similar way. Here, too, it has been mandated that personal data may only be processed subject to the data protection provisions applicable under EU law.[61] Despite that, the Fifth Money Laundering Directive provides for unlimited data disclosure. Whether restrictions to the contrary – such

57 ECJ judgement of 16 December 2008, C-73/07 (Satamedia), Sammlung Beck 2008, I-9831; ECtHR, judgement of 27 June 2017, 931/13, NLMR 2017, 264.

58 Recital 22 f. to Directive 2011/16/EU (fn. 59 below).

59 Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (OJ EU L 64/1 of 11 March 2011).

60 For information on how the GDPR relates to the Data Protection Directive 95/46/EC, see D.II.3 below (p. 76).

61 See recital 42 to the Fourth Money Laundering Directive (Directive (EU) 2015/849 of 20 May 2015, OJ EU, 5 June 2015, No L 141/73) and recital 38 to the Fifth Money Laundering Directive (Directive (EU) 2018/843 of 30 May 2018, OJ EU, 19 June 2018, No L 156/43).

as exemptions for minors and individuals at risk from crime – will be sufficient to meet data protection requirements seems doubtful, however.

Given the vaguely defined criteria in the Directive and the range of interpretation of the basic data protection rights on which they are based, the task of finding an appropriate balance between these conflicting requirements will largely fall on the judiciary and ultimately the ECJ.[62] Before we investigate this issue in section D, we intend first to assess the existing disclosure requirements.

62 See Fuchs/Lakenberg, "Das Transparenzregister nach dem neuen Geldwäschegesetz", NJW-Spezial 2017, 463 (464).

C. Assessment of existing disclosure requirements

Before the legal review of the burdens relevant under data protection law imposed on companies and natural persons in section D can be performed, an assessment is required of the existing disclosure requirements. A comprehensive analysis of all disclosure requirements affecting economic activity would, however, go beyond the remit of this document and does not seem necessary, as the preliminary considerations about the methodology have shown (see I.). The main point at issue is the especially serious intrusion resulting from the disclosure of data to the general public. These types of disclosure requirements have a long tradition in commercial and business law, although the recent introduction of the transparency register has given them a whole new quality (see II.). In tax law, the principle of transparency vis-à-vis the tax authorities has always applied, but so far, there has never been a requirement for universal disclosure; here, too, a paradigm shift is in the making (see III.). All these disclosure requirements taken as a whole are therefore relevant for data protection (see IV.). This is because, from the perspective of protecting the party concerned, it is not each individual requirement, which in isolation may be acceptable, but the overall image that third parties could piece together from the data that is publicly accessible.

I. Preliminary considerations about the methodology

Given the plethora of disclosure and publication requirements, a careful selection is required of the obligations with the greatest impact. In this process, disclosure requirements must be clearly distinguished from transparency requirements (see 1.). In addition, there is a need first to conduct preliminary considerations about the methodology on which the assessment of the negative impact on companies can then be based. It should be assumed in this context that the analysis will be conducted across several areas of the law (see 2.). The detailed analysis of the individual rules will then require a look at whether and to what extent individual legal provisions are required to remove information asymmetries (see 3.), for whom the information is feasibly intended (see 4.) and what it covers (see 5.).

1. Disclosure and transparency requirements

In particular, discussions about legal policy often fail to distinguish properly between transparency and disclosure requirements.[63] We cannot find fault with this state of affairs from a legal perspective, because neither term has been given an accurate definition. But, according to the opinion put forward in this document, a clear definition could contribute significantly to greater accuracy in capturing the legal problems at the root of these two terms. This study defines disclosure requirements exclusively as the requirement to provide information to the general public, or at least to a subset of the public, for

63 One example is the critical opinion of the Deutsches Aktieninstitut, which devotes the section entitled "Transparenz bei der Unternehmensbesteuerung" (Corporate taxation transparency) to the planned public country-by-country reporting, although strictly speaking this relates to tax disclosure (Deutsches Aktieninstitut, Kurvenlage, first half of 2018, p. 66, https://www.dai.de/files/dai_usercontent/dokumente/jahresbericht/2018-I%20Kurvenlage.pdf).

example in cases where data is ready for download from a freely accessible register. The definition of transparency requirements is much broader; it refers to all reporting and action requirements to make company or personal data accessible to the authorities. The number of transparency requirements relating to companies is almost impossibly large, because companies are subject to reporting requirements in probably every area of business, tax and administrative law (e.g. the requirement to file tax returns). This shows that disclosure requirements are a subset of the significantly more extensive transparency requirements. The particularly intense manner in which they interfere with basic rights justifies treating them separately. The publication of personal data is conceivably the most serious interference with basic rights, because the subsequent use of the data can no longer be controlled. At any rate, in practice, this renders moot the prohibition on changing the purpose of using the data and, similarly, procedural guarantees, such as the obligation to delete, review and provide information on the affected data, will be virtually impossible to enforce.

2. Analysis across several areas of the law

Disclosure requirements have their origins in highly divergent areas of the law; they are intended for different users and serve different objectives. The legal analysis of disclosure requirements normally deals with the issues according to their classification into specific areas of the law. This classification must be left to one side for the purpose of this study, because the study is aimed at facilitating a legal assessment of the overall burden on companies resulting from disclosure requirements and of the need to protect individuals who have to disclose personal data. For this kind of assessment, the area of the law in which the disclosure requirement has originated is irrelevant.

This is why we will present an analysis of what are currently the most significant disclosure requirements under commercial and business law. The study only looks into those disclosure requirements that apply to any commercial enterprise, irrespective of the sector in which it operates. There is no scope here for addressing the particularities of companies that, due to the nature of their activities, are subject to special regulation (for example credit institutions and insurance undertakings). In the area of tax, the perspective has been widened to include new information requirements vis-à-vis the authorities, because in terms of legal policy this issue is closely related to the public country-by-country reporting being planned by the European Commission.

3. Removal of information asymmetries through the imposition of disclosure requirements

Most information is distributed unevenly, and very little information is known to everyone. Since information often arises in a particular place or in the sphere of a particular individual or company, the imbalance of information between different persons is, in a sense, the normal state of affairs. In some areas, the imbalanced distribution of information may make transactions dysfunctional: A contract is imbalanced in substance because one party knows more than the other; a company is inefficiently managed because the Board of Management does not provide frank information to the Supervisory Board – to name but two examples.

Economic law analysis uses the term "information asymmetry" to describe the problem highlighted here.[64] While the neoclassical model assumed a comprehensively informed market participant in its considerations, the new institutional economics turned to the problem of transaction costs – the cause of which can, in good part, can be attributed to information asymmetries. Since the distribution of information is imbalanced, the acquisition of information always involves costs, which get in the way of an efficient transaction. Market failure is one of the consequences that can often be observed when the market mechanism is, by itself, unable to ensure an adequate supply of information.[65] In this way, binding information rules can be justified from a legal and economic perspective, as long as they elicit information that is useful for decision-making and reduce transaction costs.[66] Government's role in this context is to facilitate the supply of information to the market and tailor it to the needs of the users of the information. This is a key justification for instituting the commercial register and the binding legal norms it entails.[67]

However, not all information asymmetries entail a need for legal regulation, because market failure is by no means found everywhere. A bank customer applying for a loan will give the bank the requested information voluntarily, while a listed stock corporation would sometimes prefer to leave its small shareholders in the dark about certain transactions. Other types of information attributable to private individual or companies may be considered worth knowing by third parties – but the legal system does not allow them any legally protected interest in the information. Examples include the private affairs of a natural person or business secrets belonging to a company. In such cases, the parties concerned could even obtain an injunction against the dissemination of such information. In other cases, the dissemination of information is in the public interest, and those affected cannot prevent it from being published (e.g. press reports on the poor performance of companies that could have a negative impact on the economic situation of the region, or reports on the personal misconduct of politicians, who have to accept a public interest in them as individuals).

There are, however, legal requirements that go one step further in that they force the holders of the information to disclose it themselves to third parties or the general public (e.g. publication of the annual financial statements of corporations). Such a legal requirement, which is imposed on citizens against their will and may well compromise their interests, requires substantive justification under the rule of law. There has to be a legitimate interest in the information to justify interference with individual freedom.

---

64 Detailed discussion with additional references: Merkt (fn. 6), p. 207 ff.

65 Merkt (fn. 6), p. 217 ff.

66 See Merkt (fn. 6), p. 224 ff.: "analytical view of the functions" of disclosure rules.

67 Knieper, *Eine ökonomische Analyse des Notariats*, 2010, S. 52 f.

4. Information user group

A key criterion for selecting the disclosure requirements under investigation is the group of users that obtain access to the information disclosed. For example, it makes a big difference if personal information (e.g. an individual's personal income) has to be disclosed specifically to the competent authority (e.g. the tax office), or whether the public at large can get hold of the information unfiltered (e.g. the salaries of members of the board of management of listed companies).

The group of users at which the information is addressed matters because it provides a clue to the legal justification of the disclosure requirement. For example, the reporting requirements imposed on corporations because of their limited liability primarily serves to protect creditors. This has an effect on the legal structure, scope and intensity of the reporting requirement and on the type of information to be disclosed. The situation is similar in capital markets law, which focuses on the investors as the users of the information.

5. Content of the information to be disclosed

Of key importance for the legal review is therefore the nature of the information to be disclosed. The release of company data is typically less serious than the disclosure of personal data. There is also a difference in the criteria applied when weighing up the interests of the affected party. When disclosing company data, the prime concern of the company in question is that it may incur a competitive disadvantage, if competitors are able to use the information to their advantage. Private individuals, by contrast, generally enjoy legal protection of their personal data and privacy, and any disclosure has to be specifically justified in the light of this protection.

II. Disclosure requirements under commercial and business law

Disclosure requirements have a long tradition in commercial and business law: their emergence can be traced to the beginning of the modern era and the introduction of commercial registers. The most significant obligations in legal practice will be explained first in an analysis of the status quo (see 1.). As a summary, this will dovetail into an analysis that outlines, among other things, the scope of data protection law, which is often overlooked in the traditional debate about commercial and business law (see 2.). The study will then proceed to take a more in-depth look at this aspect.

1. Analysis of the status quo

The analysis of the status quo of disclosures under commercial and business law leads from legacy disclosure types, such as the company name and commercial register (see a), and disclosure requirements specific to the legal form, which are governed by the laws regulating German limited liability companies (GmbHs; see b) and stock corporations (see c) through modern developments in the publication of annual financial statements (see d) and capital markets transparency (see e) down to the most recent

developments, which include the introduction of the transparency register (see f and g), the German Transparency in Wage Structures Act (see h) and the AnaCredit Regulation (see i).

a) Disclosure requirements under commercial law

aa) Commercial name disclosures (sections 17 ff. of the HGB)

The merchant's commercial name is the name it uses in legal transactions (see 17 (1) of the HGB). Its purpose is to identify the natural or legal person(s) responsible for running the business and provide information on liability.[68] In Central Europe, evidence of the functions of the commercial name, in particular in relation to the law of commercial partnerships, can be found as far back as the 16th and 17th centuries.[69]

Since the reform of commercial law in 1998, merchants are largely free in the choice of their commercial name,[70] i.e. the name does not necessarily have to contain the name of its owner; the commercial name may also make reference to the purpose of the business or even be freely invented. This freedom is limited by the prohibition on misleading commercial names (section 18 (2) of the HGB).

Key criteria for the selection of the commercial name are identifiability and the ability to distinguish it from others (section 18 (1) of the HGB) to ensure that the specific commercial business can be properly identified in legal transactions. In addition, the commercial name must provide information about the allocation of liability (see section 19 of the HGB). This is expressed through extensions to the commercial name such as OHG, KG, GmbH & Co. KG, GmbH or AG. The commercial name must be entered in the commercial register (section 29 of the HGB) and in this way made accessible to everyone (see section 9 of the HGB). It must also be quoted in all business correspondence (section 37a of the HGB).[71]

The clear identification of the commercial name is required in the interest of legal transactions and in the interest of those wishing to enter into legal relationships with the merchant, partnership or company. Moreover, its business partners have a legitimate right to be informed about the allocation of liability. The purpose of commercial name law is thus to pursue regulatory objectives as well as to lay down rules to protect individuals.

---

68 Merkt (fn. 6), p. 32.

69 Merkt (fn. 6), p. 33.

70 K. Schmidt, *Handelsrecht*, 6th ed. 2014, p. 446 ff.

71 Today business correspondence also includes electronic communication, especially e-mail (Hopt in: Baumbach/Hopt, *Handelsgesetzbuch*, 38th ed. 2018, section 37a, marginal note 4).

bb) Disclosures in the commercial register (sections 15 ff. of the HGB)

Commercial register disclosures have a long tradition. In the 13th century in northern Italy, registers started to be kept with information about merchants; these registers could be used to obtain details about business partners.[72] Over the centuries, this information increasingly took on a public disclosure function in the sense that the merchant could only rely on registrable facts in dealings with third parties if these facts were entered in the register.[73]

Today, European Union law sets out important conditions for the commercial register and the impact it has. The Disclosure Directive of 1968 governed the establishment of commercial or company registers and the information they were required to include.[74] The provisions of this directive have meanwhile been subsumed in the consolidated directive on company law.[75] Although the directive only governs the law of corporations (GmbH, AG and KGaA),[76] German legislators additionally implemented the provisions that were already in line with its own commercial law tradition and expanded in particular the provisions governing the effect of registration pursuant to section 15 of the HGB to cover all merchants.[77] Regulations that deal specifically with the GmbH, KGaA or AG were included in the German Limited Liability Companies Act (GmbH-Gesetz) and the German Stock Corporation Act (Aktiengesetz; see b and c below).

In general, anyone carrying on a trade (within the meaning of sections 1 ff. of the HGB) must file certain information on this trade in the commercial register. In addition to the commercial name, a business address in Germany is required at which any legal documents can be served on the merchant. Commercial partnerships have to provide the surname, first name, date of birth and place of residence of each partner and their authority to represent the company (section 106 (2) of the HGB). For partnerships limited by shares, the registration must include the limited partners as well as their contributions (section 162 of the HGB).

The commercial register provides information that allows the entity's owner to be identified and, if necessary, legally significant notifications to be served on that person effectively. The commercial register also contains information on the allocation of liability. In addition, any person can access the annual

72 Jutzi (fn. 1), p. 416; Merkt (fn. 6), p. 35 ff.

73 Merkt (fn. 6), p. 37 ff.

74 Council Directive of 9 March 1968 (68/151/EEC), OJ EC, 14 March 1968, No L 65/8.

75 Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017, OJ EU, 30 June 2017, No L 169/46. Here specifically Art. 16 (Disclosure in the register) and Art. 14 (Documents and particulars to be disclosed by companies).

76 See Annex II to Directive 2017/1132.

77 See Bayer/J. Schmidt, in: W. Bayer/M. Habersack (eds.), *Aktienrecht im Wandel*, vol. I, 2007, chapter 18, marginal note 20 (p. 958).

financial statements of corporations submitted to the register. This information serves the legitimate interests of business partners and creditors, especially those of businesses organised in the legal form of corporations with limited liability. It also helps to cut transaction costs, because the time and expense required to get the information are reduced considerably.

Statutory provisions ensure that the information in the commercial register is accessible to any person (section 9 (1) sentence 1 of the HGB). There is no need to demonstrate a legitimate interest.[78] In the Daihatsu ruling, the European Court of Justice confirmed the will of European legislators of making the disclosed information accessible to "any interested party".[79] Data protection considerations were evidently not deemed important when the group of potential users was extended. As a countermeasure, German legislators intended to take data protection requirements into account by restricting access to "information purposes".[80] The specialist literature took a critical view of this restriction, arguing that its legitimate use could be derived from the legal requirement to disclose the information.[81]

The debate was triggered by a case on which the Federal Court of Justice (Bundesgerichtshof, BGH) ruled in 1989: a commercial enterprise had requested access to the commercial register in order to transfer its entire content onto microfilm and use it to create an information system on a private commercial basis. The BGH ruled that the right to access to the information in the register did not extend to this project.[82] Although this right was not restricted to single entries and also included the right to make individual copies of the information accessed, a copy of the entire contents in order to create a private commercial system that competes with the commercial register was "something essentially different". This kind of access would far exceed what had been intended in section 9 (1) of the HGB.

The enterprising trader's private initiative could certainly be welcomed as a sensible response to the shortcomings of government red tape,[83] because the commercial register, which was still kept on paper at the time and could only be accessed on request, was not especially user-friendly. Any attempt to connect the data with the aim of increasing its informative value therefore had to contend with considerable practical

78 Hopt in: Baumbach/Hopt (fn. 71), section 9 marginal note 1.

79 ECJ, case C-97/96, ECLI:EU:C:1997:581, marginal note 22.

80 Government draft of a law on electronic registers and legal costs for telecommunications, BT-Drs. 14/6855, p. 17 (explanatory memorandum to section 9 of the HGB new version).

81 Hirte, "Kommerzielle Nutzung des Handelsregisters", CR 1990, 631 ff.; Noack, "Online-Unternehmensregister in Deutschland und Europa", BB 2001, 1261, (1262 ff.).

82 BGH, IVa ARZ (VZ) 9/88, BGHZ 108, 32 (36).

83 Hirte (fn. 81) (635).

hurdles.[84] However, this aspect is rightly irrelevant in the case being considered. What matters is that the BGH – without naming it as such – paid respect to the important principle of purpose limitation in data protection law: i.e. that data the law requires citizens to disclose may subsequently only be used for the purpose for which it was originally requested. The collection and use of the data for private commercial purposes is not the purpose for which the merchant has submitted this data to the commercial register.

In any case, it is much easier today to access the data than at the time the above BGH ruling was handed down. The commercial register is now kept online and can be accessed at www.handelsregister.de by any person at any time. In addition, the business register has been introduced (section 8b of the HGB) to implement European regulations, which require that corporate data is recorded in "a single file"[85]. This register is also available online to anyone (www.unternehmensregister.de). In addition to the details from the commercial register, it also contains data from the cooperative societies register and the register of partnerships of the liberal professions, for example. In addition, documents that must be submitted pursuant to section 325 of the HGB (see d below) are made available through the business register.

It would probably be quite difficult to compile a personal profile by aggregating data from the business register relating to a specific individual, because it is not yet possible to conduct keyword searches among the data records. The search is launched using certain index data specified in the German Business Register Regulation (Unternehmensregisterverordnung, URV),[86] including the commercial name and legal form as well as its registered office and address (section 6 of the URV). No provision has been made to allow searches for individuals, so it is not possible to browse for specific persons in a systematic way.[87] It makes sense to build in this hurdle from a data protection perspective, because it makes it more difficult to link up personal information, which could then be used for purposes that are entirely unconnected to the protection of creditors and business partners.

b) German Limited Liability Companies Act

As a trading entity (section 13 (3) of the GmbHG), limited liability companies (GmbH) are subject to the same disclosure requirements as all other merchants under commercial law. The disclosure requirements explained under a) above therefore also apply to GmbHs. The German Limited Liability Companies Act also sets out other provisions, which supplement the disclosure requirements under commercial law. The

84 It is particularly for this reason that Hirte argues in favour of commercial use by private service providers, because this can help reduce information costs for third parties; from a data protection perspective, only a link to other registers would be questionable, not the optimal use of the register concerned (Hirte (fn. 81), (634)).

85 Art. 16(1) sentence 1 of Directive (EU) 2017/1132 of 14 June 2017, OJ EU, 30 June 2017, No L 169/46.

86 See Seibert/Wedemann, "Der Schutz der Privatanschrift im elektronischen Handels- und Unternehmensregister", GmbHR 2007, 17, (20).

87 Seibert/Wedemann (fn. 86) (20).

following section will consider these provisions, with special focus on the personal data of shareholders and managing directors.

When a GmbH is established, evidence authenticating the managing directors and a list of shareholders must be submitted for entry in the commercial register (section 8 (1) nos. 2 and 3 of the GmbHG). Subsequent replacements of managing directors must also be notified (section 39 of the GmbHG), and the list of shareholders must be kept up to date at all times (section 40 of the GmbHG). The list must provide the surname, first name, date of birth and place of residence of the shareholders as well as the nominal amounts and serial numbers of the shares they have acquired and the percentage of the share capital they hold as a result (section 40 (1) sentence 1 of the GmbHG). Their private addresses do not have to be provided in the list of shareholders, although in practice they are sometimes included.[88]

When the company is registered, information on the identities of the managing directors must also be submitted (section 10 (1) sentence 1 of the GmbHG). Details are governed by the German Commercial Register Regulation (Handelsregisterverordnung, HRV). Section 43 no. 4b of the HRV requires the entry of each managing director's surname, first name, date of birth and place of residence. The director's private address does not have to be disclosed. Together with information about the authority to represent the company (section 10 (1) sentence 2 of the GmbHG), the data entered serves to provide assurance in legal transactions with a GmbH about the individuals authorised to issue legally effective statements on behalf of the company. The disclosure of the managing directors' identities gives effect to the public disclosure function of the commercial register; it means that third parties can confidently expect that the managing directors entered there are authorised to represent the company.[89] The business correspondence of a GmbH has to give details of all managing directors, including their surnames and at least one first name in long form; if the GmbH has a supervisory board, the name of its chairperson must also be specified (section 35a (1) of the GmbHG).

The list of shareholders, which has to be submitted for inclusion in the commercial register, provides transparency about shareholder structures. This requirement was included by German reform legislators in 2008 in response to recommendations by the Financial Action Task Force on Money Laundering to combat money laundering and terrorism financing.[90] In combination with the newly created circumstance of bona fide acquisition of shares from a person lacking authority (section 16 (3) of the GmbHG), this

88 Seibert/Wedemann (fn. 86) (19).

89 This, too, serves to implement European requirements (see Art. 8 of Directive (EU) 2017/1132 of 14 June 2017 relating to certain aspects of company law, OJ EU, 30 June 2017, No L 169/46).

90 BT-Drs. 16/6140, p. 37: explanatory memorandum to amendments to section 16 of the GmbHG.

was additionally intended to ensure a higher degree of legal certainty for the transfer of GmbH shares in a chain of assignment, which may be very long in some cases.[91]

The above disclosure rules of the German Limited Liability Companies Act therefore pursue different regulatory objectives: On the one hand, they continue the tradition in commercial law of providing the kind of information needed in legal transactions that allows such transactions to be conducted with legal certainty. This helps to reduce transaction costs. On the other hand, the amendments to the rules applying to the list of shareholders pursue a separate, mainly public-interest objective: the transparency is intended to prevent criminal offences (money laundering and terrorism financing) and make it easier to solve such crimes. This additional legal policy objective can be achieved without additional effort in the law governing limited liability companies, because the creation and publication of the list of shareholders is required in any event to meet the above-mentioned intentions under commercial and company law.

However, as soon as the disclosure requirement ceases to be tied to the position of shareholder, we leave the domain of the law governing limited liability companies. This happens, at least in part, in the transparency register, which has its justification not in company law, but seeks to identify "beneficial ownership". The economic position, in contrast, is irrelevant under the law governing limited liability companies, because it does not entail any legal consequences under company law. The section on the transparency register will analyse this problem more closely (see f below).

c) German Stock Corporation Act

In the same way as GmbHs, stock corporations (Aktiengesellschaft, AG) are by law trading entities (section 3 (1) of the AktG); this means they are subject to general disclosure requirements under commercial law. The additional requirements of the German Stock Corporation Act are analysed below, with special focus on the disclosure of personal data.

aa) Personal data relating to the founders

When a stock corporation is established, its articles of association must be adopted by way of a notarial deed (section 23 (1) of the AktG). The articles of association must be appended to the registration in the commercial register (section 37 (4) no. 1 of the AktG). The "founders" must be specified in the articles of association document (section 23 (2) no. 1 of the AktG). The founders are those shareholders who adopted the articles of association and acquired at least one share (see section 28 of the AktG).[92] They have to be specified as such in the articles of association in such a way that they can be clearly identified; it is a widely held view that, for natural persons, this means disclosure of their first names and surnames

91 BT-Drs. 16/6140, p. 38: explanatory memorandum to amendments to section 16 of the GmbHG.

92 Limmer in: G. Spindler/E. Stilz (eds.), *Kommentar zum Aktiengesetz*, 3rd ed. 2015, section 23 marginal note 25; Seibt in: K. Schmidt/M. Lutter (eds.), *Aktiengesetz*, 3rd ed. 2015, section 23 marginal note 25.

as well as their addresses.[93] The background to this requirement is the liability of the founders (section 46 of the AktG), which can only be enforced if the founders can be identified.[94] Information on the founders' identity is not required as part of the entry in the commercial register (see section 39 (1) of the AktG), but may be found by third parties by looking up the articles of association filed in the register.

An interesting question from a data protection perspective is whether the founders' private addresses are required to identify them. The literature on company law often affirms this requirement;[95] however, there are also arguments to the contrary, which rightly question the need for disclosing the founders' private addresses.[96] The purpose of this requirement is to allow the founder to be clearly identified – in case a claim is made. However, in normal circumstances it is possible with reasonable effort to identify an individual clearly on the basis of their first name and surname and place of residence.[97] When analysed systematically, this view is confirmed in the provision of section 43 no. 4b of the HRV, which was discussed earlier in connection with managing directors of limited liability companies (GmbHs): According to this provision, the place of residence is sufficient for identifying managing directors of limited liability companies. Parties entering into legal transactions have an equally substantial interest in reliably establishing their identities, but their private addresses are not included in the entry.

bb) Personal data relating to members of executive bodies

When filing for registration of a stock corporation in the commercial register, the documents relating to the appointment of the board of management and the supervisory board must also be appended (section 37 (4) no. 3 of the AktG). Members of the board of management are also entered in the commercial register (section 39 (1) sentence 1 of the AktG): similarly to the requirement for managing directors of limited liability companies, the surname, first name, date of birth and place of residence must be entered for each member of the board of management (section 43 no. 4b of the HRV).

The registration filing must be accompanied by a list of supervisory board members (section 37 (4) no. 3a of the AktG), providing the surname, first name, profession and place of residence of each member (section 37 (4) no. 3a AktG). Their private addresses do not have to be disclosed.[98] The names of supervisory board members are not entered in the commercial register (see section 39 of the AktG), but

93 Limmer in: Spindler/Stilz (fn. 92), section 23 marginal note 25; Seibt in: Schmidt/Lutter (fn. 92), section 23 marginal note 25.

94 Seibt in: Schmidt/Lutter (fn. 92), section 23 marginal note 25.

95 See with additional references Limmer in: Spindler/Stilz (fn. 92), section 23 marginal note 25.

96 Seibert/Wedemann (fn. 86) (19).

97 Seibert/Wedemann (fn. 86) (19).

98 Kleindiek in: Schmidt/Lutter (fn. 92), section 39 marginal note 5.

details of the individuals who are members of the supervisory board can be determined by accessing the list submitted with the commercial register filing.

The business correspondence of stock corporations has to give details of all members of the board of management and of the chairperson of the supervisory board, including his or her surname and at least one first name in long form (section 80 (1) sentence 1 of the AktG).

cc) Identifying the shareholders

Although the founders of a stock corporation have to be personally identifiable (see above), this does not apply to shareholders who acquire interests subsequently. Unlike partnerships – where the information is required for allocating liability (section 106 (2) no. of the 1 HGB for partners with unlimited liability, section 162 (1) of the HGB for limited partners) – the shareholders of a stock corporation (AG) are not entered in the commercial register. Nor does the German Stock Corporation Act specify a list of shareholders (as is required for GmbHs), providing the company has not issued any registered shares (more on that later).

Notifications to the company under stock corporation law are only required when a shareholder breaks through the threshold of holding more than 25 per cent of the shares (section 20 (1) sentence 1 of the AktG); the next threshold that triggers a notification requirement is when a majority interest is acquired (section 20 (4) of the AktG). If the interest held drops below one of the above-mentioned thresholds, the company must likewise be notified (section§ 20 (5) of the AktG). According to the express wording of the act, the notification requirement applies only to "business entity"; it therefore does not affect private shareholders.[99] Stock corporations that receive a notification as mentioned above have to publish it in newspapers authorised to publish this information (section 20 (6) of the AktG); this always includes publication in the Federal Gazette (section 25 of the AktG). If the company finds out about a qualifying interest in any other way, it is not required to publish this information; the company is also not required to conduct its own research.[100] In view of these restrictions, the provisions set out in section 20 of the AktG contribute little to making the shareholdings in a stock corporation transparent.

Up until the stock corporation law reform of 2016, shareholders were able enjoy anonymity outside the scope of section 20 of the AktG if the company had issued bearer shares, because these shares are transferred by handing the share certificates from one shareholder to another.[101] The company is usually

99 Veil in: Schmidt/Lutter (fn. 92), section 20 marginal note 13. A private shareholder is considered to be someone who only has this one shareholding and does not hold shares in other companies (representative example: Court of Appeal (Kammergericht, KG) in Berlin, case ref. 14 AktG/1/10, AG 2010, 494 (496)).

100 OLG Stuttgart, 20 AktG 1/12, AG 2013, 604 (608).

101 Raiser/Veil, Recht der *Kapitalgesellschaften*, 6th ed. 2015, p. 122. For information on transfers by assignment, see Bezzenberger in: Schmidt/Lutter (fn. 92), section 68 marginal note 6.

not aware of these transactions. This is different for registered shares, for which the shareholder's name, date of birth and address, as well as the number of shares or share numbers, must be entered in the company's share register (section 68 (1) sentence 1 of the AktG). The shareholder is required to notify the company of this information (section 68 (1) sentence 2 of the AktG). In relation to the company, only a person who is entered in the share register is considered a shareholder (section 68 (2) sentence 1 of the AktG). The legal mechanism is similar to that used for the list of shareholders for GmbHs (see b above).

Whether a stock corporation issues bearer shares or registered shares is determined by its articles of association (section 23 (3) no. 5 of the AktG). Traditionally, there has been a preference for bearer shares in Germany, with registered shares only being used where it was important to the company to know its shareholders (e.g. in family companies).[102] However, legal policy makers are becoming increasingly distrustful of bearer shares, claiming that it is difficult to combat money laundering and terrorism financing if the board of management of a stock corporation can respond to a request by saying that it does not know the identity of the shareholders and is under no legal obligation to know them.[103] The opacity of the shareholdings has exposed Germany to international criticism.[104] The stock corporation law reform of 2016 therefore regulated the use of bearer shares more tightly,[105] with a distinction between listed and unlisted companies.[106]

Listed companies may continue to use bearer shares (section 10 (1) sentence 2 no. 1 of the AktG), because capital markets law requires shareholdings to be transparent in any case (see e below). Companies whose shares are not exchange-traded may, however, only issue bearer shares if the issuance of individual certificates has been excluded and a global share certificate is deposited with a central securities depository or another authorised custodian (section 10 (1) sentence 2 no. 2 of the AktG). This rules out the previously allowed practice of anonymously purchasing shares by merely acquiring possession of the share certificate. The record of the transfer transaction can be used to identify the seller and the buyer due to the special nature of the global share certificate, which represents all shares; the actual share transfer merely requires a booking process.[107] However, the shareholder does not deal with

102 Raiser/Veil (fn. 101).

103 According to the explanatory memorandum to section 10 of the AktG, new version, included in the government draft to amend the German Stock Corporation Act, BT-Drs. 18/4349, p. 16.

104 The Financial Action Task Force (FATF) and the G8 summit had strongly recommended the appropriate adjustments (see government draft to amend the German Stock Corporation Act, BT-Drs. 18/4349, p. 15 f.).

105 See Harbarth/Freiherr von Plettenberg, "Aktienrechtsnovelle 2016: Punktuelle Fortentwicklung des Aktienrechts", AG 2016, 145 (146).

106 According to the legal definition of section 3 (2) of the AktG, companies are deemed listed on a stock exchange if their shares are admitted to a market that is regulated and supervised by government-approved authorities and that is directly or indirectly accessible to the public.

107 Bezzenberger in: Schmidt/Lutter (fn. 92), section 68 marginal note 11 ff.; Raiser/Veil (fn. 101), p. 122.

the securities depository directly, but indirectly via a custodian bank.[108] People who want to buy bearer shares represented by a global share certificate cannot do so without a securities account.[109] In this way, transparency can be created at least for government authorities wishing to investigate suspicious transactions: The identity of the shareholder can be established by submitting a request to the institution managing the securities account.[110]

d) Publication of annual financial statements

aa) Corporations (section 325 of the HGB)

Corporations have to publish their annual financial statements, the management report and the auditor's report (section 325 (1) sentence 1 no. 1 of the HGB). In addition to the balance sheet, the annual financial statements include the income statement (section 242 (3) of the HGB). Moreover, corporations have to supplement the annual financial statements with notes that constitute an integral part of the balance sheet and the income statement (section 264 (1) sentence 1 of the HGB). The annual financial statement and management report must subsequently be audited by an auditor (sections 316 ff. of the HGB). The auditor is required to discharge his or her duty impartially and without bias.[111] The audit of the financial statements is therefore a "key building block" in the system of disclosure requirements.[112]

The adopted and approved annual financial statements, the management report and the auditor's report (or non-affirmative auditor's report) must be filed electronically with the operator of the electronic Federal Gazette in a format that allows their publication (section 325 (1) of the HGB). These provisions also apply, with the necessary modifications, to the filing and publication of consolidated financial statements and group management reports (section 325 (3) of the HGB).

The requirement to publish annual financial statements applies to all corporations (AG, KGaA, GmbH). Partnerships are exempted, providing they have at least one personally liable partner who is a natural person (section 264a of the HGB). The GmbH & Co. KG, which is popular among small and medium-sized enterprises, is required to publish annual financial statements, because the GmbH – as the general partner – is not a natural person.

108 Bezzenberger in: Schmidt/Lutter (fn. 92), section 68 marginal note 12.

109 Ziemons in: Schmidt/Lutter (fn. 92), section 10 marginal note 47.

110 Harbarth/Freiherr von Plettenberg (fn. 105) (147).

111 For a representative example see BGH, II ZR 49/01, BGHZ 153, 32, 43.

112 Luttermann/Großfeld, *Bilanzrecht*, 4th ed. 2005, p. 470.

Requirements to publish annual financial statements are graded according to size:[113] "Small" corporations are only required to disclose the balance sheet and the notes (section 326 (1) of the HGB), and are exempt from the audit requirement (section 316 (1) sentence 1 of the HGB). A corporation is considered "small" if it does not exceed two of the following three criteria (section 267 (1) of the HGB): total assets of €6 million; sales of €12 million; 50 employees. "Micro-corporations" benefit from an additional practical expedient: they have to file only the balance sheet (section 326 (2) of the HGB). This category covers companies that do not exceed at least two of the following three criteria (section 267a (1) of the HGB): total assets of €350,000; sales of €700,000; ten employees. "Medium-sized" corporations are allowed to file a balance sheet that has been abridged according to specified criteria (see section 327 of the HGB). A corporation is considered "medium-sized" if it exceeds at least two of the three criteria of a "small" corporation and at the same time does not exceed two of the following three criteria: total assets of €20 million; sales of €40 million; 250 employees (section 267 (2) of the HGB). A corporation is considered "large" if it exceeds at least two of the three criteria just mentioned (section 267 (3) of the HGB).

bb) Partnerships and sole traders (German Public Disclosure Act)

Sole traders and partnerships in which at least one partner has full liability are generally not required to prepare or file annual financial statements. This exemption from the disclosure requirement is justified by the personal liability of the owner or partner. Under the German Public Disclosure Act, special arrangements apply, however, to entities that exceed certain indicators. In the same way as corporations, they have to prepare annual financial statements (section 5 (1) of the PublG), have them audited by an auditor (section 6 (1) of the PublG) and then publish them (section 9 (1) of the PublG).

The German Public Disclosure Act applies to entities that meet at least two of the following three criteria (section 1 (1) of the PublG) as at the day on which a financial year ends and as at each of the two subsequent balance sheet dates: total assets of more than €65 million reported in the annual balance sheet as at the balance sheet date; sales of more than €130 million in the twelve months prior to the balance sheet date; more than 5,000 employees on average in the twelve months prior to the balance sheet date.

cc) Regulatory objectives

The requirement to publish annual financial statements has traditionally been justified with reference to creditor protection.[114] There is also an opposing view that public disclosure results in damage rather than advantages and that it mainly benefits competitors, even though creditors can also protect them-

113 In terms of the definitions explained below, sales are calculated for the twelve months prior to the balance sheet date and the number of employees is the annual average (see sections 267, 267a of the HGB). The legal consequences of the size classification only apply if the criteria are exceeded or fall below the limit in two successive financial years (sections 267 (4), 267a (1) sentence 2 of the HGB).

114 Hommelhoff, "Europäisches Bilanzrecht im Aufbruch", RabelsZ 62 (1998), 381; Merkt (fn. 6).

selves on an individual basis.[115] But this does not alter the fact that the existing legal provisions pursue the intention of protecting creditors, at least as far as the legislator is concerned. The requirement to publish annual financial statements is based on the EU Accounting Directive. In its recitals, the scope of the directive (AG, GmbH, GmbH & Co. KG) is explicitly justified by the fact that the reporting entities are "limited liability companies" that do not offer third parties any security beyond their net assets.[116]

In the Springer case, this approach was put before the European Court of Justice for review.[117] A newspaper publishing house had invoked its professional and press freedom to justify its refusal to disclose its annual financial statements. As reasons, it pointed out that, once disclosed, the annual financial statements were accessible not only to creditors, but to anyone, without the need to demonstrate a legitimate interest.[118] However, the ECJ allowed this wide range of application of the disclosure requirement, arguing that it has been laid down in the definition of powers in Art. 54(3)(g) TEC (today Art. 50(2)(g) TFEU). It was therefore permissible that anyone had the opportunity, on the basis of the directive, to access the annual financial statements and management reports of the company forms included in the scope without having to demonstrate a legitimate right or interest.[119] The ECJ saw the logic of the directive in balancing the benefits of limited liability that some company forms enjoy against adequate disclosure to protect the interests of third parties.[120] If this was interpreted as having a negative effect on professional freedom, this effect was "clearly justified".[121]

The German Public Disclosure Act of 1969 pursues a different regulatory objective. Given the kind of owners to which it applies (sole traders and partnerships), the disclosure requirement cannot be regarded as a correlate of limited liability. Rather, the entities to which the German Public Disclosure Act applies have to disclose their annual financial statements "regardless of their legal form".[122] In this case, legislators saw the function of public disclosure in "the economic interest derived from the ability to draw conclusions for macroeconomic development on the basis of the data provided by major companies".[123] This was because the fortunes of a major business had an effect on the interests of a large number of

115 Bachmann/Eidenmüller/Engert/Fleischer/Schön, *Rechtsregeln für die geschlossene Kapitalgesellschaft*, 2012, p. 152.

116 Directive 2013/34/EU, OJ EU, 29 June 2013, No L 182/19, recitals 3 and 5.

117 ECJ, joined cases C-435/02 and C-103/03 (Springer), 24 September 2004, ECLI:EU:C:2004:552.

118 See ECJ, ibid., marginal note 21

119 ECJ, ibid., marginal note 35.

120 ECJ, ibid., marginal note 68.

121 ECJ, ibid., marginal note 49.

122 Explanatory memorandum to government draft, BT-Drs. 5/3197, p. 13.

123 Explanatory memorandum to government draft, BT-Drs. 5/3197, p. 13.

third parties and often their existence as well.[124] These third parties include suppliers and customers, employees, lenders and investors and all the agents who have to make economic and social policy decisions with an impact on the company.[125] The interest of all the parties involved, and therefore that of the public, outweighed any opposing interests of the owners.[126] Their obligation to face the criticism of the financial press and thus the general public meant that they had to take particular care when making investment and financing decisions.[127]

dd) Weighing up public disclosure against companies' legitimate interests

As we have just seen, the legitimate interests of the companies affected cannot be used as an argument against the disclosure requirement. But they do carry weight if the data disclosed is used for commercial purposes[128] or if derogatory public statements are made on the basis of this data. For example, the BGH instructed a professor of economics to refrain from using the annual financial statements of a construction company, all of whose shares were family-owned, as a case study in a commercial seminar presented to more than 900 people; he had also named the company in the process.[129] In his presentation, the professor concluded that a critical view should be taken of the company's financial situation.[130] According to the BGH, that was a violation of the general right of personality,[131] because the naming of the company in question affected its need for social recognition as an employer and a commercial enterprise. The fact that the annual financial statements had already been published and were therefore known to interested groups could not be used as a counterargument. The analysis before an audience with expert knowledge had the effect of highlighting the matter and drawing attention specifically to data that could lead to a critical assessment.[132] Although the publication of annual financial statements was intended to protect third parties, it did not give third parties the right to use a company "for their own gainful purposes" and to name the company in the process.[133] The protection of the professor's academic freedom was no

124 Explanatory memorandum to government draft, BT-Drs. 5/3197, p. 13.

125 Explanatory memorandum to government draft, BT-Drs. 5/3197, p. 14.

126 Explanatory memorandum to government draft, BT-Drs. 5/3197, p. 14.

127 Explanatory memorandum to government draft, BT-Drs. 5/3197, p. 14.

128 See the ruling on the commercial use of commercial register data mentioned in fn. 82 above.

129 BGH, 8 February 1994, VI ZR 286/93, AG 1994, 222.

130 BGH, ibid., AG 1994, 222.

131 BGH, ibid., AG 1994, 222, 223.

132 BGH, ibid., AG 1994, 222, 223.

133 BGH, ibid., AG 1994, 222, 223.

justification for this course of action. He could have pursued his academic interests without any serious limitations by redacting the company's name and address beforehand.[134]

The Federal Constitutional Court refused to accept a subsequent constitutional complaint lodged by the professor.[135] It argued that no violation of the constitution could be detected in weighing up opposing positions under constitutional law. The test applied was set out in article 2 (1) of the GG, which also protected free development in terms of economic activity. The complainant had been unable to demonstrate why it was crucial for the objective of the seminar to reveal the plaintiff's name and address.

Both rulings were criticised – in some cases sharply – in the specialist literature on business law:[136] they had missed the purpose of the disclosure requirements. It was feared that lawyers, tax advisers and investment advisers would in future be unable to warn their clients of companies in financial difficulties, because they would have to reveal their names in the process. It was also expected that the financial press would in future be unable to form an opinion on the basis of having studied annual financial statements and to report on them subsequently.[137]

The criticism of the rulings seems exaggerated, since in its decision the BGH followed a path that can be clearly justified from a data protection perspective. Personal or company-related data may only be used for the purpose for which it was originally made available. This is the same reason why, in the 1989 ruling mentioned earlier, a private commercial enterprise was told it could not transfer the entire contents of the commercial register onto microfilm and use it to create its own register for commercial gain. It was argued that access to the commercial register was not granted for the purpose of commercial gain.[138] This line of reasoning was followed in the professor's case, even though, for the use of the documents for educational purposes, it was at least considered whether it was really necessary to reveal the company's name: this kind of use is no longer fully compatible with the original purpose of disclosure, which is to protect those creditors and business partners that intend to establish contact with the specific company in question.

134 BGH, ibid., AG 1994, 222, 223 f.

135 BVerfG, 3 May 1994, 1 BvR 737/94, AG 1994, 369.

136 Lutter, "Die handelsrechtliche Publizität – direkt für die Mülltonne?", AG 1994, 363; Mertens, "Anm. zur BVerfG-Entscheidung", AG 1994, 370.

137 For supporting arguments, see Lutter (fn. 136).

138 BGH, IVa ARZ (VZ) 9/88, NJW 1989, 2818 (2820).

From an EU law perspective, we should bear in mind that EU legislators intended to protect third parties from the financial risks associated with limited liability company forms.[139] Although there is no obligation to demonstrate a legitimate interest in order to gain access, this does not necessarily mean that the subsequent use of the data is not subject to any legal barriers. The data has not been provided for the user's own commercial gain. In this case, therefore, the affected company's legitimate interests would outweigh those of the other party, and the data should be anonymised where this can reasonably be expected. In the case of a commercial seminar, this can be done without significantly impairing its functions. When advising a client who is to be warned against establishing a business relationship with a company in financial trouble, the process of weighing up interests has a different outcome. Here the information interests of the third party for whose protection the directive was adopted clearly outweigh the interest of the company in question in keeping its identity secret. The fact that the courts arrived at a considered balance against the interests of the affected party is therefore compatible with the purpose of the disclosure requirements.

e) Capital markets transparency

The disclosure requirements under capital markets law are particularly far-reaching, and are often regarded as paradigmatic of the whole body of company disclosure law.[140] The scope of application of capital markets law relates to markets rather than companies; it regulates securities trading on legally organised markets.[141] Securities include in particular the shares of a stock corporation (see section 2 (1) no. 1 of the WpHG). Typical family companies – the group that is relevant in this case – are not very likely to fall within the scope of capital markets law. At most, it is feasible that a small portion of the shares will be made available for trading, while the family continues to hold the majority. Since the issue of debt securities, such as bonds, will also lead to the application of capital market regulations, at least in part (see section 2 (1) no. 3 of the WpHG), we want to discuss these instruments below to the extent necessary.

aa) Prospectuses (German Securities Prospectus Act)

The publication of a securities prospectus when issuing securities is governed by the German Securities Prospectus Act (Wertpapierprospektgesetz, WpPG). At the European level, this act is based on the EU Prospectus Directive, which will soon be replaced by the EU Prospectus Regulation (see Art. 49 Prospectus

---

139 ECJ, joined cases C-435/02 and C-103/03 (Springer), 24 September 2004, ECLI:EU:C:2004:552, marginal note 50.

140 The fundamental studies by Merkt and Jutzi deal with capital markets law as a prime example of company disclosure: Merkt (fn. 6), p. 296 ff.; Jutzi (fn. 1), p. 72 ff.

141 It is not possible to provide a more detailed definition of the scope of capital markets law in this document. See instead: Buck-Heeb, *Kapitalmarktrecht*, 9th ed. 2017, p. 21 ff.; Klöhn in: K. Langenbucher (ed.), *Europäisches Privat- und Wirtschaftsrecht*, 4th ed. 2017, p. 335 ff.; Zetzsche/Eckner in: M. Gebauer/C. Teichmann (eds.), *Europäisches Privat- und Unternehmensrecht*, 1st ed. 2016, p. 658 ff.

Regulation on the effective dates of most of its provisions in 2019).[142] The Prospectus Directive has been expanded by a regulation adopted by the European Commission, which is referred to by section 7 of the WpPG.[143]

A securities prospectus must be prepared if securities are to be offered publicly or admitted to trading on a regulated market (see section 1 of the WpPG). The prospectus serves to inform potential investors about the issuer and the securities being offered (see section 5 (1) of the WpPG): Investors are meant to be able to form an appropriate opinion of the assets and liabilities, financial situation, profits and losses and future prospects of the issuer. For this reason, the information provided in the prospectus must be presented in a format that is easy to analyse and understand. Pursuant to section 13 of the WpPG, the prospectus requires the approval of the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin). It must then be published in one or more widely circulated business or daily newspapers and on the issuer's website (section 14 (2) of the WpPG).

The securities prospectus requires issuers of securities to disclose a broad range of company-related information. Annex I to the regulation adopted by the European Commission itemises, for example, the most significant past and future investments, significant new products, a description of the most important markets and an explanation of the corporate structure. Although this is the kind of economic data on which investors focus, some disclosures of personal data are also required, such as the names and addresses of the following individuals:[144] members of the board of management and supervisory board; personally liable partners of a KGaA; founders, if the company has been established for fewer than five years; and members of senior management authorised to determine the fact that the issuing company has suitable expert knowledge and suitable experience to manage the business activities of an issuer. If there are family relationships between these individuals, this information must also be provided. Other details that require disclosure include information on previous management positions in other companies, any criminal convictions or bankruptcies and personal remuneration. Finally, the name and address of the issuer's auditor must be provided.

bb) Ad-hoc disclosures (MAD)

Once the securities have been issued, the issuer is required to publish ad-hoc disclosures on an ongoing basis. The legal basis of this requirement is the European Market Abuse Directive (MAD).[145] The disclo-

142 Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003, OJ EC, 31 December 2003, No L 345/64; Regulation (EU) 2017/1129 of the European Parliament and of the Council, OJ EU, 30 June 2017, No L 168/12.

143 Commission Regulation (EC) No 809/2004 of 29 April 2004, OJ EU, 30 April 2004, No L 194/1.

144 See Annex I items 14.1, 15.1 of the Prospectus Regulation adopted by the European Commission.

145 Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014, OJ EU, 12 June 2014, No L 173/1.

sure requirement relates to inside information, defined as information of a precise nature which has not been made public, relating, directly or indirectly, to one or more issuers or to one or more financial instruments, and which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments[146] (see Art. 7(1)(a) MAD). The issuer must make this information public without undue delay (Art. 17(1)(1) MAD).[147]

Non-public information that is likely to have an effect on the price of a financial instrument is often of a corporate nature. The examples given in BaFin's Issuer Guideline include the disposal of core businesses, the acquisition of major holdings, the default of significant debtors or important inventions.[148] Personal data may be subject to the disclosure requirement, if it could potentially affect the price; however, this will only be the case in exceptional circumstances. The Guideline lists "unexpected changes in key positions held within the company".[149] The Daimler/Geltl case drew a lot of attention in this context: a shareholder accused the company of informing the public too late of the impending resignation of its CEO, Jürgen Erich Schrempp.[150]

cc) Shareholding transparency (WpHG)

Investors holding voting shares in a listed company can influence the company by exercising their voting rights. The WpHG lays down rules to ensure shareholding transparency so that other investors can find out who has significant influence over the company. Anyone who reaches, exceeds or falls below of the thresholds of three per cent, five per cent, ten per cent, 15 per cent, 20 per cent, 25 per cent, 30 per cent, 50 per cent or 75 per cent must inform the issuer of the securities and BaFin without undue delay (section 33 (1) sentence 1 of the WpHG). This means that there is much greater transparency of shareholdings for listed than for unlisted stock corporations (see under c above).

To ensure that the reporting requirement cannot be undermined, section 34 of the WpHG contains a number of attribution rules. For example, the calculation to determine whether a threshold has been reached includes the voting rights of a subsidiary of the reportable entity or those held by a third

146 The definition of financial instrument is broader than that of security, but does include the shares and bonds that are relevant here (see Annex I section C of Directive 2014/65/EU, to which Art. 3 no 1 MAD makes reference). See Buck-Heeb (fn. 141), p. 96.

147 The original version, which had read "as soon as possible" was subsequently changed into the correct legal phrase "without undue delay" (see OJ EU, 21 December 2016, No L 348/83 (85)).

148 Issuer Guideline of the Federal Financial Supervisory Authority, 4th ed. (German only), 2013, p. 53 (can be found at www.bafin.de, where an English translation of the 3rd ed. is available).

149 Issuer Guideline (fn. 148), p. 53.

150 ECJ, case C-19/11, ECLI:EU:C:2012:397. Representative examples dealing with the problem of "protracted processes" in Klöhn, "Das deutsche und europäische Insiderrecht nach dem Geltl-Urteil des EuGH", ZIP 2012, 1885 ff. and Zetzsche in: Gebauer/Teichmann (fn. 141), p. 833 ff. (section 7 marginal note 110 ff.).

party for the account of the reportable entity. In recent years, some cases attracted attention when companies succeeded in acquiring a considerable interest in other companies without having to report this in advance (stake-building by stealth).[151] This was achieved with the help of different derivative financial instruments whose economic effect was that the reportable entity was offered voting shares when the derivatives matured. Legislators reacted by amending sections 25 and 25a of the WpHG; the provisions have since been incorporated into section 38 of the WpHG.[152] The result is a high standard of shareholding transparency which provides justification for exempting listed stock corporations from the transparency register regulations (see f below).

dd) Disclosure of board remuneration

There was protracted wrangling over the disclosure of board remuneration among legal policy makers.[153] For this kind of personal data, the public's interest in the information must be weighed against the affected party's right to data privacy. Accounting law therefore generally only requires disclosure of the total remuneration of all members of the board of management (section 285 no. 9. a) of the HGB). If in exceptional circumstances the total remuneration provides information that could reveal the remuneration of a single member (e.g. if the board of management only has one or two members), the company may opt not to disclose the total remuneration (section 286 (4) of the HGB).[154] This restriction serves to protect the personal data of the board members concerned.[155]

Nevertheless, individual shareholders may attempt, at the annual general meeting, to obtain more detailed information by invoking their right to information under stock corporation law (section 131 of the AktG). The question of total board remuneration is invariably relevant for the agenda item dealing with the formal approval of the actions of the board of management and the supervisory board and therefore requires a response.[156] If the company has opted to invoke the omission option of section 286 (4) of the HGB, a separate investigation must be conducted as part of the request for information under stock corporation law to establish whether this omission was justified[157] In the past, most requests

151 See Cascante/Topf, "'Auf leisen Sohlen'? – Stakebuilding bei der börsennotierten AG", AG 2009, 53 ff.

152 See Teichmann/Epe, "Die neuen Meldepflichten für künftig erwerbbare Stimmrechte (§§ 25, 25a WpHG)", WM 2012, 1213 ff.

153 The provisions under commercial law (section 285 no. 9. a) of the HGB) also govern the remuneration of the supervisory board, advisory board or similar body. The details discussed here focus on the members of boards of management, because their remuneration is typically much higher and invariably represents the main source of income, which consequently means that the individuals concerned have a greater need for confidential treatment.

154 Lücke, "Die Angemessenheit von Vorstandsbezügen – Der erste unbestimmbare unbestimmte Rechtsbegriff?", NZG 2005, 692; Spindler, "Das Gesetz über die Offenlegung von Vorstandsvergütungen – VorstOG", NZG 2005, 689.

155 Bundestag Legal Affairs Committee, BT-Drs. 12/7912, p. 23.

156 OLG Düsseldorf, 19 W 2/97 AktE, AG 1997, 520.

157 See OLG Düsseldorf (fn. 156) (521), where the shareholder's request for information was successful.

for disclosure of individual remuneration were rejected based on the argument that this information is not necessary for a decision about whether to approve the actions of the board of management and the supervisory board.[158] If information is requested on the remuneration of one management level below the board of management, the amount of total remuneration will be disclosed at most, but not individual salary levels.[159] According to the OLG in Frankfurt, this does not constitute a violation of the right to data privacy, because the total amount of remuneration cannot be used to determine individual remuneration.[160]

Legal policy makers have been demanding the disclosure of individual board remuneration for many years, especially for listed companies, claiming it would make management oversight by shareholders more effective, because it would allow them to make a connection between a board member's personal performance and his or her remuneration,[161] and could possibly have a dampening effect on the sometimes excessive salary levels.[162] In the case of listed companies, it would be a way of informing potential investors (who do not have the right to pose such questions under section 131 of the AktG) about the incentive and governance structures of the company.[163] All these arguments apply in particular to listed companies, because their shareholders typically have less detailed information from the company than, say, those of a family company organised as a stock corporation and are therefore especially reliant on mandatory reporting requirements. However, since information provided under capital markets law is, by its nature, accessible to any person, privacy protection can very rarely be achieved by channelling the information. Any disclosures required for the benefit of investors will inevitably also reach the general public.

In view of the above-mentioned oversight functions, it has meanwhile become an explicit requirement for listed stock corporations to disclose board remuneration on an individualised basis.[164] Section 285 no. 9. a) sentence 5 HGB requires, for listed stock corporations, the separate disclosure of "the remuneration of each individual member of the executive board [...], giving his or her name, classified into non-performance-related components and long-term incentive components". There is no provision for situation-based exemptions for reasons of privacy protection. These disclosures may only be omitted

158 Representative example in LG Berlin, 98 AktE 10/89, AG 1991, 34 (36). Further references in Spindler in: Schmidt/Lutter (fn. 92), section 131 marginal note 48.

159 OLG Frankfurt, 20 W 56/05, AG 2006, 460 (461).

160 OLG Frankfurt (fn. 159) (462).

161 Representative example in Baums, "Zur Offenlegung von Vorstandsvergütungen", ZHR 169 (2005), 299 (300 ff.).

162 Arguing this point e.g. Hoffmann-Becking, "Rechtliche Anmerkungen zur Vorstands- und Aufsichtsratsvergütung", ZHR 169 (2005), 155 (173).

163 In turn, see Baums (fn. 161) (306 ff.).

164 For information on its development, see Gurman, *Die Vorstandsvergütung nach der Finanzkrise,* p. 116 ff.

if this has been resolved by the general meeting (section 286 (5) sentence 1 of the HGB). Pursuant to general rules under stock corporation law, a simple majority is sufficient to pass such resolutions (section 133 (1) of the AktG). Even then, it is sometimes argued that individuals could obtain information on individual remuneration by invoking their right to information (section 131 of the AktG).[165]

The disclosure of the salaries of board members in listed companies is a good example of how data, once published, takes on a life of its own in the public debate. Investors and shareholders do use the information for the purpose intended by legislators when they imposed the disclosure requirement: they use the salary debate as a basis for interrogating the management performance of the board of management. If they have been satisfied with its performance, they will accept a high salary. The general public, in contrast, engages in a completely different kind of debate, in which the mere fact that board members earn significantly more than the average citizen meets with their disapproval. Reports on board salaries can then be found under headings such as "heads of DAX-listed companies amassing fortunes" – illustrated with a picture of a luxury yacht with the caption "the millionaires' favourite toy". [166] The criterion of remuneration commensurate with company performance, which is relevant for shareholders, takes on a very minor role in the public's perception.

It could be argued that publicly exposed persons, such as board members in major companies or politicians, have to live with the fact that they will not be handled with kid gloves in public. But this experience should make us take a cautious approach with trends that any shareholding can be used to justify demands for disclosure to the general public, as is the case with the transparency register right now. We will revisit this aspect in the overall assessment (see IV. below).

ee) CSR reporting

Since 2017, the amendments contained in section 289b to 289e of the HGB have specified the inclusion of a "non-financial statement" in the management report.[167] Based on the underlying philosophy of a socially responsible company, this is also referred to as "corporate social responsibility statement", or "CSR statement" for short. The HGB provisions governing the CSR statement were included to implement EU Directive 2014/95, which inserted a new Art. 19a in the Accounting Directive (EU Directive 2013/34).[168]

165 Spindler in: Schmidt/Lutter (fn. 92), section 131 marginal note 48 (with reference to opposing view).

166 http://www.fr.de/wirtschaft/vorstandsverguetung-dax-chefs-mit-goldenen-nasen-a-1473523.

167 The requirements are applicable for the first time to annual and consolidated financial statements and management and group management reports for financial years beginning after 31 December 2016 (Art. 80 of the German Act Introducing the German Commercial Code).

168 Directive 2014/95, 22 October 2014, OJ EU of 15 November 2014, No L 330/1.

The non-financial statement relates in particular to aspects of environmental protection, employee matters, social matters, respect for human rights and anti-corruption (section 289c (2) of the HGB). In the opinion of EU legislators, disclosure of non-financial information is a key element in managing change towards a sustainable global economy by combining long-term profitability with social justice and environmental protection.[169] The reporting requirement "helps the measuring, monitoring and managing of undertakings' performance and their impact on society". The reporting requirement serves as a "procedural transmission belt" to manage companies' behaviour and encourage them to act responsibly.[170]

The provisions do not prescribe how companies have to realise CSR matters, they merely have to report on them. A company is even allowed not to have any policies at all in relation to one or more CSR matters, but in that case, a "clear and reasoned explanation" must be provided for not doing so (section 289c (4) of the HGB). Ultimately, many of the companies affected will formulate a positive commitment to CSR to serve their own reputational interests. It may, however, take a lot of work to produce such a report, at least for companies that have not had any CSR policy in the past.[171]

The requirement to file a non-financial statement applies to large corporations (within the meaning of section 267 (3) of the HGB; see d) above) that are publicly traded (within the meaning of section 264d of the HGB) and have more than 500 employees on average throughout the year (section 289b (1) sentence 1 of the HGB). To ease their bureaucratic burden, small and medium-sized enterprises (SMEs) are not subject to this requirement.[172] At first glance, the reporting requirement seems to be a special obligation applicable to major companies, reflecting their economic and social importance.[173] Yet CSR reporting can become an additional burden even for SMEs, because the major companies to which it applies will invariably have to comment on compliance with the CSR standards in their supply chains in order to demonstrate that they have plausible CSR policies. For this reason, they will impose documentation requirements and quality processes on their suppliers so they can show their CSR commitment in a credible manner.[174] One of the typical ways of enforcing such standards is to pass them to suppliers along the supply chain.[175]

---

169 Directive 2014/95, recital 3.

170 Simons, "Corporate Social Responsibility und globales Wirtschaftsrecht", ZGR 2018, 316 (318 f.).

171 Hennrichs, "Die Grundkonzeption der CSR-Berichterstattung und ausgewählte Problemfelder", ZGR 2018, 206, 208, points out that little is likely to change for some DAX companies, because they have already reported on CSR matters on a voluntary basis in the past.

172 Directive 2014/95, recitals 13 and 14.

173 Fleischer, "Corporate Social Responsibility", AG 2017, 509 (517).

174 Hennrichs (fn. 172) (210).

175 Simons (fn. 171) (320).

f) Transparency register (GwG)

aa) Scope of application

The transparency register was introduced by the new German Money Laundering Act (Geldwäschegesetz, GwG) as at 26 June 2017. It records the "beneficial owners" of companies organised as legal entities under private law or as registered partnerships. The transparency register was introduced in compliance with the Fourth EU Money Laundering Directive of 20 May 2015 (hereinafter "MLD 2015").[176] This directive has already been amended and reformed again by the Fifth Money Laundering Directive of 30 May 2018 (hereinafter "MLD 2018").[177] Pursuant to Art. 4 MLD 2018, national legislators have until 10 January 2020 to transpose the amended directive. The current legislation, which will be discussed first, is therefore still based on MLD 2015, which German legislators will have to amend in line with MLD 2018 in the course of 2019.

bb) Concept of "beneficial owner"

Beneficial owner means any natural person who ultimately "owns or controls" a legal entity or registered partnership (section 3 (1) no. 1 of the GwG). Pursuant to section 3 (2) sentence 1 of the GwG, a beneficial owner is any natural person who directly or indirectly owns more than 25 per cent of the capital stock. Furthermore, a beneficial owner is anyone who controls more than 25 per cent of the voting rights or exercises control in a comparable manner. This does not necessarily have to involve a natural person. If the direct shareholder of a company is a legal entity, the true beneficial owner must be determined along the chain of ownership interests.

cc) Reporting requirements

The legal reporting requirements for the transparency register have been imposed on the company itself. Legal entities under private law and registered partnerships have to collect and retain the required information on the beneficial owner, keep it up to date and report it to the office keeping the register (section 20 (1) sentence 1 of the GwG). In addition, the act lays down an obligation for shareholders to provide the required information without undue delay. This requirement applies to "shareholders who are beneficial owners or are under the direct control of the beneficial owner" (section 20 (3) of the GwG). The company is then required pursuant to section 20 (1) sentence 1 of the GwG to disclose this information to the transparency register. For a GmbH, the reporting requirement is deemed to have been met if the identity of the beneficial owner can be derived from the list of shareholders (section 20 (2) of the GwG).

dd) Third-party access

Based on the current version of the GwG, the transparency register can be accessed not only by government authorities, but by any third party, providing it can demonstrate to the office keeping the register

176 Directive (EU) 2015/849 of 20 May 2015, OJ EU, 5 June 2015, No L 141/73.

177 Directive (EU) 2018/843, 30 May 2018, OJ EU of 19 June 2018, No L 156/43.

that it has a legitimate interest in accessing the information (section 23 (1) sentence 1 no. 3 of the GwG). Examples include specialised journalists wanting to research aspects of money laundering.

The arrangements for accessing the register are governed by a regulation (TrEinV).[178] Access can be gained through the website, www.transparenzregister.de (section 1 (1) of the TrEinV). Persons authorised to access the register (pursuant to section 23 (1) of the GwG) must register as users. This requires them to enter a user ID in the form of a valid e-mail address and assign a password (section 2 (3) of the TrEinV). Once the user account has been activated, data relating to the identity of the user must be submitted (section 2 (4) of the TrEinV). If the user is not a natural person, the e-mail address and telephone number of the natural person instructed to effect the registration must be provided (section 2 (4) no. 2 letter d of the TrEinV). In addition, proof of identity is required; suitable methods include a copy of an identity document, for example (section 3 of the TrEinV).

If the user subsequently submits an application to gain access, he or she has to demonstrate a legitimate interest in accessing the register. For non-governmental organisations, eligible documents are the articles of association, if they reveal that the organisation is engaged in work to counter money laundering and terrorism financing, while specialised journalists can present research planned or already conducted in the area of money laundering and terrorism financing (section 8 of the TrEinV). The application must specify for which organisation pursuant to section 20 (1) of the GwG or for which legal structure pursuant to section 21 (1) and (2) of the GwG and for which period the user requests access to the register (section 5 (2) of the TrEinV). To prevent abuse, the office keeping the register must keep a record of which user has accessed which data in the transparency register and when it was accessed (section 10 (1) of the TrEinV).

The office keeping the register must delete the application record, including the confirmation or demonstration of the right to access, without undue delay two years after the decision relating to the application was taken (section 5 (3) of the TrEinV). Likewise, the record of the data relating to the specific access must be deleted without undue delay two years after access (section (3) of the TrEinV). There is no provision for informing the organisation or beneficial owner concerned. This means the affected parties will, under normal circumstances, not be informed when specific data has been accessed or when the information necessary for any follow-up has been deleted.

ee) International scope of application

The rules governing the transparency register apply to the corporate and other legal entities incorporated within the territory of each Member State (Art. 30(1) MLD 2015).[179] It therefore does not really help the

178 Transparenzregistereinsichtnahmeverordnung (German Regulation on Inspection of the Transparency Register), 19 December 2017, BGBl. I p. 3984.

179 This passage has not been amended by MLD 2018.

beneficial owner of a company entered in the register in Germany if only the German legislators apply all the available data protection options to protect the affected individuals. If a company entered in the register in Germany establishes a subsidiary in another EU Member State, this subsidiary is subject to the national law of the country in which it is entered. This means that information about the beneficial owner must be disclosed – along the entire chain of ownership interests – in accordance with the provisions of anti-money laundering law applicable there. The data registered in other Member States is not limited to users domiciled in the Member State keeping the register. Ultimately, this means that the lowest level of data protection law will prevail among the EU Member States.

g) Amendments to the Money Laundering Directive (2018)

aa) Considerations of the European Commission

Very shortly after MLD 2015 was adopted, the European Commission saw further need to revise the legal requirements for combating money laundering and terrorism financing. On 5 July 2016, it therefore submitted a proposal to reform the Money Laundering Directive.[180] For the problematic aspects of disclosure requirements that are the subject of this study, the key question is whether the transparency register will in future be openly accessible to any person.

The European Commission argued that if any person could have access to the register, this would provide additional guarantees for third parties wishing to do business with a company.[181] Complex owner structures had in practice been used to camouflage criminal activities, tax liabilities and the involvement of politically exposed persons and persons subject to sanctions.[182] Knowledge about the beneficial owners was a basic prerequisite for minimising risk in connection with financial crime and for prevention strategies adopted by regulated companies.[183] It also maintained that the protection of minority shareholders and other stakeholders necessitated access to reliable information about ownership structures.[184] In addition, public access would allow better control of the information by civil society, including the press and civil society organisations.[185] If everyone who went into business with a legal entity was informed about the identity of the beneficial owner, this could simplify investigations and have reputational effects, which would in turn contribute to fighting abuse of legal entities and legal arrangements.[186]

---

180 European Commission, *Proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 and amending Directive 2009/101/EC*, 5 July 2016, COM(2016) 450 final.

181 European Commission, COM(2016) 450 final, p. 13.

182 European Commission, COM(2016) 450 final, p. 18.

183 European Commission, COM(2016) 450 final, p. 18 f.

184 European Commission, COM(2016) 450 final, p. 19.

185 European Commission, COM(2016) 450 final, p. 19.

186 European Commission, COM(2016) 450 final, p. 19.

The European Commission also commented on the extent to which public access to the data was compatible with Articles 7 and 8 of the Charter of Fundamental Rights and the principle of proportionality. The European Commission believes that proportionality is maintained because unlimited disclosure requirements only apply to commercial enterprises, and that access should remain restricted for legal entities or trusts not aiming to make a profit.[187] It also pointed out that the existing rules, according to which the Member States were required to define the conditions in which a "legitimate interest" in accessing the register existed, were at risk of creating inconsistent access to information that differed from country to country.[188] The European Commission conceded that the regulatory concept under which access to the register was linked to demonstrating a legitimate interest had been created for reasons of data and privacy protection. However, the freedom this granted to the Member States allowed them to create different levels of transparency – ranging from excessive access restrictions at one end to unlimited disclosure at the other.[189]

The European Commission stressed that it had specifically made the Member States aware of the fact that they would have to pay particular attention to the principle of proportionality, to data protection and to the protection of the right to privacy.[190] Member States would have to ensure in this context that access by third parties pursued an objective of general interest and that the necessity and proportionality of potential restrictions of the protection of personal data and the right to privacy were fully established.[191] Whether the amendments to the Money Laundering Directive meet the European Commission's own data protection requirements will be the subject of the analysis below.

bb) Regulatory options for access to the transparency register

In preparation for the reform of the directive, the European Commission considered two regulatory options:[192]

The first option was to continue to leave it for the Member States to decide the level of disclosure, i.e. not to depart from MLD 2015 on this point. This would, however, not change anything in terms of the disparate levels of information among the Member States.[193]

187 European Commission, COM(2016) 450 final, p. 8.

188 European Commission, Impact Assessment, SWD(2016) 223 final, p. 100.

189 European Commission, Impact Assessment, SWD(2016) 223 final, p. 100.

190 European Commission, Impact Assessment, SWD(2016) 223 final, p. 100.

191 European Commission, Impact Assessment, SWD(2016) 223 final, p. 100.

192 European Commission, Impact Assessment, SWD(2016) 223 final, p. 100.

193 European Commission, Impact Assessment, SWD(2016) 223 final, p. 100.

The second option was to amend the Directive by making it mandatory to give full public access rights to the information. This would make the legal framework more consistent and allow more efficient research on the beneficial owner.[194] It would increase the transparency of legal entities and allow the data to be scrutinised by civil society.[195] This would benefit anyone wishing to do business with the company or legal entity.[196] The rights of the persons affected were sufficiently protected by allowing exemptions from the disclosure requirement in justified exceptional circumstances; that related to situations where disclosure would expose the beneficial owner to the risk of falling victim to crime.[197]

cc) Critical assessment

The European Commission's arguments are unconvincing for two reasons:

(1) The European Commission assumes different levels of information among the Member States without providing any evidence. It is unable to provide this evidence for the simple reason that, when the amendments were drafted, MLD 2015 had not even been implemented in all the Member States.

(2) The The European Commission limits the assessment of potential consequences to only two options, without even mentioning an obvious third option, which would have been to lay down the criteria for weighing information and data protection interests in the EU directive itself.

Central to the European Commission's line of argument is the assumption of different information levels in the Member States. It was argued that this could be derived from the regulatory freedom MLD 2015 gave the Member States, who could set their own criteria for determining when a "legitimate interest" in accessing the register existed. The European Commission arrived at the view that this would create an information differential between the Member States that was unacceptable for the single market at a time when MLD 2015 had not yet been transposed into national law in the Member States. It mentioned in its assessment of the consequences that there was little information available on existing practices in the Member States related to beneficial ownership data. It attributed this to the fact that the Money Laundering Directive 2015 had not yet been transposed.[198] The reasons provided do not reveal why it would not have been possible to wait for the implementation of MLD 2015 in order to analyse its practical impact thereafter. The argument that different levels of information among the Member States were

194 European Commission, Impact Assessment, SWD(2016) 223 final, p. 102.

195 European Commission, Impact Assessment, SWD(2016) 223 final, p. 101.

196 European Commission, Impact Assessment, SWD(2016) 223 final, p. 101.

197 European Commission, Impact Assessment, SWD(2016) 223 final, p. 100 f.

198 European Commission, Impact Assessment, SWD(2016) 223 final, p. 102.

feasible was not based on the facts determined, but merely describes the regulatory concept agreed when MLD 2015 was adopted.

The European Commission emphasised that there had been valid reasons for adopting the provisions of MLD 2015. The aim had been to do justice to data protection and the protection of the right to privacy. Again, no reasons were supplied for assuming that the protection of data and the right to privacy weigh less now than at the time MLD 2015 was adopted. Reference to the exemption in the case of potential crime threats does not meet these justification requirements, because this exemption already exists in MLD 2015. The removal of the "legitimate interest" requirement scales back data protection and the protection of the right to privacy without offering any explanation for assuming that the need required under MLD 2015 to consider both sides has become redundant.

The argument that Member States would possibly apply different benchmarks does carry weight. However, the problem cannot be solved by dropping the requirement to weigh it against the protection of privacy of those affected. Instead, the European Commission should have investigated a third option, which would have involved the creation of European benchmarks for considering the different interests. For example, MLD 2018 could have provided a more detailed definition of when a "legitimate interest" applies, such as a list of those interests that always justify access to the register. This would have achieved a minimum level of harmonisation, thus guaranteeing a consistent basic level of access to information. There is a more detailed discussion elsewhere in this document which argues that these fundamental assessments must be regulated at EU level and cannot be left to the discretion of Member States (see D.V.1).

Lastly, some of the arguments the European Commission uses to justify giving everyone access to the transparency register bear no relation to the fight against money laundering and terrorism financing. The European Commission maintains that minority shareholders and stakeholders could have an interest in obtaining information about the beneficial owner. It does not provide any evidence suggesting that this could be a real problem in business practice. In the debate about shareholding transparency up to that point, this claim had only been made for exchange-listed companies, where it has been implemented to a large extent by way of legislation under capital markets law. In terms of legal policy, this is based on the argument that, if there is a large number of shareholders, it is in fact almost impossible for small shareholders to understand the company's shareholder structure without outside help. In unlisted companies, the situation is normally different. Typically, their shareholders know each other personally. The European Commission does not argue that the minority shareholder of an unlisted company could have a practical need to consult a public register for information about the majority shareholder. Yet even if such a need existed, it could have been satisfied by including this group of persons in the list of individuals who have a "legitimate interest" in accessing the register. Disclosure to the general public cannot be justified in this way.

The European Commission's reasoning merely pays lip service to data protection law and the protection of the right to privacy. While it had specifically emphasised in MLD 2015 that, in determining the group of persons who have a legitimate interest in accessing the register, the public interest had to be carefully weighed against data protection needs, it has now solved the problem by simply removing the weighing-up process from the directive without putting anything in its place.

dd) Opinion of the European Data Protection Supervisor

In view of the above, the European Commission's proposal has been sharply criticised by the European Data Protection Supervisor (EDPS), and for good reason.[199] The EDPS said that the proposed amendments would extend access to information on the beneficial owner as a political tool which could be used to facilitate and optimise the enforcement of tax obligations.[200] However, the aim of the directive was to improve the toolset available for the fight against money laundering. The fight against tax evasion was already covered by other EU legislative instruments.[201] Although the purpose of combating tax evasion cited originally was no longer specifically mentioned in the Council's position, the instrument of unrestricted disclosure of information on the beneficial owner, which, according to the Commission's proposal, was to be used to pursue this objective, remained in place.[202]

The fight against terrorism and serious crime was an objective being pursued in the general interest; nevertheless, where this led to interference with the fundamental rights to privacy and data protection, the proportionality of the measures would have to be assessed.[203] The proposal would introduce new legal policy objectives, i.e. the fight against tax evasion, without clearly defining them. No explanation had been offered why measures which were acceptable to combat money laundering and terrorism financing were necessary and proportionate outside that regulatory context.[204] The lack of analysis of the means-purpose relation identified by the Data Protection Supervisor seems all the more worrisome as the purpose of the legislative act is not only to safeguard the public interest in fighting tax evasion, but additionally to serve private information interests, such as those of minority shareholders and other stakeholders.

---

199 European Data Protection Supervisor, "Summary of Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC", OJ EU, 18 March 2017, No C 85/3. The full text of the opinion (hereinafter cited as "Opinion") can be found on the Data Protection Supervisor's website (https://edps.europa.eu/sites/edp/files/publication/17-02-02_opinion_aml_en.pdf).

200 Opinion, OJ EU, 18 March 2017, No C 85/3.

201 Data Protection Supervisor, Opinion, p. 7.

202 Opinion, OJ EU, 18 March 2017, No C 85/4.

203 Opinion, OJ EU, 18 March 2017, No C 85/5.

204 Data Protection Supervisor, Opinion, p. 8.

The Data Protection Supervisor criticised the fact that the objectives of data processing were being defined with less and less clarity and that personal data was being processed for a whole number of reasons, ranging from anti-money laundering to general financial market oversight.[205] This was in conflict with the data protection principle of access to data for a clearly defined purpose and with the principle of proportionality.[206] Although the Council Position repeatedly emphasised the need for data protection, there was no sign of this intention being implemented in a concrete way.[207] In particular, there was no definition of legitimate interest in accessing information that made a recognisable reference to the regulatory objectives.[208] Finally, it had to be remembered that it was not the responsibility of private players to ensure compliance with the legal system.[209]

In view of the original regulatory objective of the directive, the Data Protection Supervisor believed that access to beneficial ownership information should have been designed in such a way that it was only granted to entities who are in charge of enforcing the law.[210] However, none of these data protection concerns were given any attention in the subsequent legislative process.

ee) Consequences of MLD 2018 for the transparency register

The current rules limiting access to persons or organisations "that can demonstrate a legitimate interest", are set out in Art. 30(5)(c) MLD 2015. The amended EU Money Laundering Directive no longer contains this limitation. Member States will have to ensure that beneficial ownership information is accessible to "any member of the general public" (Art. 30(5)(c) MLD 2018). The public will receive access to at least the name, the month and year of birth and the country of residence and nationality of the beneficial owner as well as the nature and extent of the beneficial interest held. Member States may provide for access to additional information enabling the identification of the beneficial owner. That additional information includes at least the date of birth or contact details "in accordance with data protection rules". Whether and to what extent these amendments can in fact be reconciled with European data protection principles will be assessed in greater detail below (see D.V.1).

h) German Transparency in Wage Structures Act

Employers who have more than 200 employees in the normal course of business are subject to the German Transparency in Wage Structures Act (Entgelttransparenzgesetz, EntgTranspG). This act gives

205 Data Protection Supervisor, Opinion, p. 9.

206 Data Protection Supervisor, Opinion, p. 9.

207 Data Protection Supervisor, Opinion, p. 11.

208 Data Protection Supervisor, Opinion, p. 13.

209 Data Protection Supervisor, Opinion, p. 14.

210 Opinion, OJ EU, 18 March 2017, No C 85/5.

individual employees the right to obtain information from their employers on the method used to set remuneration and on comparable remuneration within the company. The comparable remuneration must be determined in relation to persons of the other sex. Requests for information on comparable remuneration must be refused if the job in question is performed by fewer than six employees of the other sex (section 12 (3) sentence 2 of the EntgTranspG). Employees are obliged to give the works council access to the lists of gross wages and salaries. The remuneration list must be classified by sex.

Compared with the disclosure requirements investigated in this study so far, the German Transparency in Wage Structures Act represents a significantly more lenient variant of the disclosure requirement. The user group of the information is tightly limited. The information is not given to the public, but to a specific employee, who may use it to draw conclusions about the appropriateness of his or her own remuneration without being able to trace the information to the salaries of specific colleagues. The thresholds specified by law (businesses with more than 200 employees, request for information refused if the benchmark group has fewer than six members) should be adequate to ensure that the data provided is anonymised.

i) AnaCredit

The AnaCredit system was developed by the European Central Bank (ECB) to provide a better overview of credit risk in the banking system. It is based on a regulation adopted by the ECB.[211] Reports are required from all credit institutions that have their registered office or a branch in an EU Member State whose currency is the euro (see Art. 3 of the Regulation). The reports are filed with the national central bank, which in turn forwards the reportable information to the ECB.

Reports are required for all credit exposures with a total of at least €25,000 (Art. 5 of the Regulation). The counterparty's identity has to be disclosed in the report (Art. 9 of the Regulation). Reportable are only credit exposures where at least one debtor is a legal entity or is part of a legal entity (Art. 4(1)(b) of the Regulation). "Legal entity" means any entity which, under the national law to which it is subject, can acquire legal rights and obligations (Art. 1(5) of the Regulation). Loan agreements with natural persons are therefore not covered by the reporting requirement.

The legal entities affected are entitled to access the data that has been reported about them (Art. 12 of the Regulation). Although third parties do not have any access to the data, the credit institutions subject to the reporting requirement may obtain from their central banks a "subset" of the credit data collected, "to the extent allowed by the applicable legal confidentiality regime" (Art. 11(1) sentence 2 of the Regulation). They may use the data exclusively for managing credit risks and improving the quality of credit information (Art. 11(1) sentence 3 of the Regulation).

211 Regulation 2016/867 of the European Central Bank of 18 May 2016 (Regulation 2016/867), OJ EU, 1 June 2016, No L 144/44.

Similar to the German Transparency in Wage Structures Act, the AnaCredit system is a relatively lenient variant of the disclosure requirement. Measured against the regulatory objective of improving the assessment of credit risks in the banking system, it would be unreasonable to object to weighing up information and protection interests from a legal perspective. This would change if the data was to be made available to a larger group of persons, let alone the general public. In such a case, the data protection requirements and thresholds developed below (see D) for the transparency register would have to be observed.

2. Summary analysis of the disclosure requirements under commercial and business law

The disclosure requirements allocated to commercial and business law in this study can be analysed in combination from different perspectives. Firstly, for data protection analysis, it is important to distinguish between company data and personal data (see a). Secondly, from a perspective that cuts across several areas of the law, it is evident that the data protection debate in commercial and business law is significantly underdeveloped (see b). Thirdly, there are signs that the purposes pursued by other areas of the law, in particular the fight against money laundering and terrorism financing, are encroaching on disclosure requirements under commercial and business law, and this is a cause for concern procedurally as well as for data protection (see c).

a) Disclosure of company and personal data

Since the disclosure requirements under commercial and business law mainly relate to company data, the reason for legitimising its disclosure is more acceptable than in the case of personal data.

Given the limitation of liability, the disclosure of company data with the objective of creditor protection is easy to justify in respect of corporations. Although competitive disadvantages cannot be ruled out, the fact that the vast majority of companies are organised as corporations means that such disadvantages will largely cancel each other out, because the competitor will be subject to the same disclosure requirements in most cases. For the protection of small and medium-sized enterprises, the information to be disclosed is reduced along a scale, based on size. Conversely, the German Public Disclosure Act requires large companies to publish their company data, even if they are not organised as corporations.

Capital markets law requires very far-reaching disclosures of company-related data, which may even have an unfavourable effect on the company concerned. By its nature, the criterion of price relevance applied to ad-hoc disclosures also covers information that companies would prefer to keep confidential. However, as capital market disclosure correlates with the extent to which the capital market is used, it can be justified quite plausibly.

The disclosure of personal data on shareholders and members of executive bodies seems more problematic. In combination with the economic data that generally has to be published on the company, the

identification of individual shareholders and the disclosure of the investments they hold permit conclusions about the financial situation of the individual concerned and could therefore reveal information that traditionally had to be disclosed to the tax office, but not the general public. This kind of disclosure must be tested more vigorously against the benchmark of data protection requirements, which have increased steadily in recent years.

b) Protection of privacy and informational self-determination

The above summary of disclosure requirements under commercial and business law has shown that there is only a very rudimentary discussion of data and privacy protection benchmarks even when personal data is disclosed. If a problem is identified at all, the commercial and business law debate is in most cases settled by the question-begging argument that the disclosure requirement is inherently legitimate and the individuals affected therefore simply have to put up with it. This argument fails by far to utilise the armoury of data protection defences, and there is insufficient awareness of the differences between the data protection mechanisms available (see D.V.1 below).

c) Encroachment of external regulatory objectives on commercial and business law

Developments in GmbH and stock corporation law have shown in particular that that commercial and business law is increasingly used for purposes that procedurally do not belong there. For example, the identification of shareholders is of interest in commercial and company law if they assert rights or are required to meet obligations in their capacity as shareholders. The information interest of fellow shareholders and of the company is derived from specific events, for example when exercising shareholder rights at a meeting of shareholders.

This internal system of company law does not automatically justify the disclosure of the shareholders' position to the general public. This kind of claim has only been brought into the realm of company law by the debate about the fight against money laundering and terrorism financing. Models of company law regulation, such as that of the list of shareholders for the GmbH or that of registered shares for the stock corporation, are put forward in the interest of combating money laundering and terrorism financing. In terms of legal categorisation, it is always of concern if the tools of different areas of the law can no longer be distinguished clearly. From the data protection perspective, this conflation of regulatory approaches becomes particularly topical because a clear purpose is demanded for each mandatory rule; this is required so that the limits of processing and forwarding data can subsequently be determined with the same level of clarity. This problem will have to be revisited in the section on data protection law of this study (see D.V.1 below).

III. Tax-related disclosure requirements

The concept of tax publicity is virtually unknown[212] in Germany and, prima facie, almost seems to be a contradiction in terms. This is because, in Germany, tax procedure law has always been subject to the principle of tax confidentiality, whose origins can be traced back to the Prussian Income Tax Act of 1851.[213] Tax confidentiality prohibits the tax authorities from passing on to third parties any information acquired during the taxation procedure. Tax publicity, i.e. the obligation to make personal tax data publicly accessible, is conceivably the most serious interference with tax confidentiality, which is now protected by section 30 of the AO.

Although there have been exemptions from tax confidentiality for a variety of reasons, disclosure requirements in the true sense are currently still completely unknown in German tax law. However, restraint in this regard could soon be history: as mentioned briefly in the introduction, the European Commission is planning to take the country-by-country report governed by section 138 of the AO in implementing the Directive on Administrative Cooperation (Directive 2016/881/EU) in Germany and turn it into a public report. This would also affect larger family companies, requiring them to disclose their sales, among other figures, if they exceed the thresholds specified in section 138a (1) of the AO.

The discussion below will approach the topic in three steps. The starting point is a section on the basic principles of tax confidentiality (see 1.). This is followed by a summary of the exemptions from these principles, including the international exchange of information and country-by-country reporting (section 138a of the AO; see 2.). The European Commission's proposal for public country-by-country reporting is then presented on this basis (see 3.).

1. Principle of tax confidentiality

Section 30 (1) of the AO requires public officials to keep tax information secret. This requirement has a long tradition and was laid down as early as the Reich Fiscal Code (Reichsabgabenordnung, RAO) of 1919 (section 10 of the RAO)[214]. Tax confidentiality is the counterpart to the far-reaching disclosure requirements under tax law.[215] In terms of categorisation, it is a detailed aspect of the general obligation to maintain professional confidentiality, as governed by, among others, section 67 of the BBG and

212 An internet search provides visible support for this claim: a Google search (as at 7 August 2018) barely yielded 10 hits.

213 Niederdorf, *Die Bedeutung des Steuergeheimnisses für die Tax Compliance – Eine vergleichende Betrachtung zwischen Schweden und Deutschland*, 2009, p. 13.

214 Reich Fiscal Code (Reichsabgabenordnung, RAO) of 13 December 1919 (Reich Law Gazette (Reichsgesetzblatt, RGBl.) II 1993).

215 BVerfGE 67, 100 (139 f.).

similar regulations at federal state level.[216] Tax confidentiality performs a dual function. Firstly, it serves the private confidentiality interests of taxpayers and other individuals required to disclose information. However, in addition to expanding on the basic right to informational self-determination by adding a statutory definition, it also pursues a fiscal purpose. The special safeguarding of confidence in professional confidentiality is intended to encourage citizens' readiness to disclose tax-relevant matters in order to help the tax process, create a complete record of tax sources and ensure taxation in compliance with the law, including fair taxation in particular.[217] This seems expedient simply because cases that constitute criminal offences or violate accepted principles of morality have tax consequences and will therefore have to be made public.[218]

Tax confidentiality received an additional boost when the GDPR entered into force. Tax data classified as personal data within the meaning of Art. 4(1) GDPR is subject to the directly applicable GDPR (section 2a (3) of the AO),[219] which is based on the principles of transparency, strict purpose limitation and security and confidentiality of data usage (Art. 5(1)(a),(b),(c),(e) GDPR).[220] When adopting the German Act Amending the Federal War Victims Relief Act and Other Regulations (Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften)[221], German legislators made use of the option allowed by Art. 6(2) GDPR to determine more precisely the requirements for ensuring lawful data processing (Art. 6(1) GDPR) for specific units of the the tax authorities. The corresponding provisions can be found in, among others, sections 2a, 29b and 29c of the AO. The scope of the GDPR is in principle limited to living natural persons (Art. 4(1) GDPR).[222] From a legal practice perspective, it is therefore highly significant that German legislators went beyond this by extending the scope of the requirements clarifying the GDPR to include not only deceased natural persons (section 2a (5) no. 1 of the AO), but also legal persons (section 2a (5) no. 2 of the AO).

2. Exemptions

The wealth of data at the tax authorities' disposal explains why other public authorities are envious of this knowledge: they want to use tax data in discharging their own responsibilities. If this is allowed, this will not only jeopardise the privacy and confidential treatment of tax obligations, but also the fiscal

216 Drüen, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, 2013, section 30 marginal note 4.

217 BVerfGE 67, 100 (139 f.).

218 Drüen, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, 2013, section 30 marginal note 8.

219 Baum, "Datenschutz im Steuerverwaltungsverfahren ab dem 25.5.2018. Teil I: Unmittelbare Geltung der DSGVO und bereichsspezifische Regelungen in der AO", NWB 2017, 3143.

220 Recital 39 (fn. 47 above).

221 Act of 17 July 2017 BGBl. I p. 2541.

222 See recitals 14 and 27 (fn. 47 above).

purpose associated with tax confidentiality. Apart from clear-cut cases, such as a professional assassin's "tax confidentiality", any qualifications must be weighed carefully.

a) Basic principles

Pursuant to section 10 of the RAO of 1919, tax confidentiality was originally guaranteed without any limitations. Legal practice and case law had, however, recognised unwritten exemptions from this general rule for reasons including the taxpayer's prior agreement and mandatory public interest.[223] The Fiscal Code of Germany of 1977 finally codified the grounds for justification in section 30 (4), (5) and (6) of the AO. Pursuant to section 30 (4) no. 2 of the AO, the grounds for justification include in particular the argument that exemptions are expressly permitted by law. Any authorisation to disclose information must have a clear and unambiguous basis in law. There is no "requirement in principle", however, to refer to the authorisation to allow exemptions from tax confidentiality.[224]

The fact that the exemptions were finally codified marked significant progress for which there is no alternative from today's constitutional law perspective in terms of the fundamental right to informational self-determination.[225] The GDPR lays down similar requirements, since personal data may only be collected for specified, explicit and legitimate purposes (Art. 5(1)(b) GDPR).

b) General overview

There are exemptions from tax confidentiality in a large number of provisions and for a wide variety of reasons. There is never any protection for wilfully false statements by the individual concerned, which may be disclosed to the law enforcement authorities (section 30 (5) of the AO). Otherwise, the disclosure and use of protected data is only permitted if the criteria of section 30 (4) nos. 1-5 of the AO are met. With due regard to the enabling clause written into German federal law, which expressly permits exemptions from tax confidentiality (section 30 (4) no. 2 of the AO), limitations on the right to tax confidentiality in excess of the list of criteria set out in section 30 (4) nos. 1 and 3-5 of the AO can only be imposed if numerous provisions under tax and non-tax law are considered as a whole.

The use of protected data is permitted for, among other purposes, implementing other tax proceedings, in criminal proceedings for tax crimes or administrative fine proceedings for administrative tax offences (section 30 (4) no. 1 of the AO), if, in specific circumstances, it serves the institution of criminal proceedings for a crime other than a tax crime (section 30 (4) no. 4 of the AO), with the consent of the person

223 See Albers, in: Hübschmann/Hepp/Spitaler/Söhn, *Abgabenordnung, Finanzgerichtsordnung*, 2004, section 30 marginal note 136.

224 Drüen, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, 2013, section 30 marginal note 71; FG Düsseldorf, judgement of 1 July 1986, VIII 446/81 AO, EFG 1986, 541.

225 See Albers, in: Hübschmann/Hepp/Spitaler/Söhn, *Abgabenordnung, Finanzgerichtsordnung*, 2004, section 30 marginal note 136 f.

concerned (section 30 (4) no. 3 of the AO) and if there is a compelling public interest in such disclosure (section 30 (4) no. 5 of the AO).

The Fiscal Code of Germany contains provisions that expressly permit the disclosure of data within the meaning of section 30 (4) no. 2, including section 31 of the AO (disclosure of tax bases), section 31a of the AO (disclosure for the purpose of countering unlawful employment and the misappropriation of benefits), section 31b of the AO (disclosure for the purpose of countering money laundering and terrorism financing), section 116 of the AO (reporting tax crimes), sections 117-117c of the AO (international legal and administrative assistance in tax matters) and section 138a of the AO (country-by-country reporting – CbCR). The provisions relating to the international exchange of information, including CbCR, is the focus of the following section (see c immediately below). Provisions on the international exchange of information in acts other than the AO can primarily be found in the German Financial Accounts Information Exchange Act (Gesetz zum automatischen Austausch von Informationen über Finanzkosten in Steuersachen, FKAustG). The most significant non-tax provisions permitting exemptions from tax confidentiality are grouped together in section 30 no. 7 of the AEAO of 2014.[226]

c) International exchange of information

The significance of the international exchange of information has increased considerably in recent years.

aa) Basic principles

The concrete underlying issue is the "disconnect between the substantive universality and the formal territoriality" of national tax law.[227] National tax law normally also imposes tax obligations on income realised abroad. For example, taxpayers with unlimited tax liability under the world income principle (section 1 (1) of the EStG in conjunction with sections 8 and 9 of the AO), which applies in Germany, have to declare their entire world income for tax purposes, not only the income generated in Germany. Since under the international territoriality principle the borders of the territory also demarcate the territorial limits for exercising state sovereignty, tax authorities are not authorised to conduct any investigations outside their national borders. This means that the tax authorities can only obtain the information required for assessing foreign taxable income in cooperation with the taxpayers or through an international exchange of information.[228]

If taxpayers refuse to cooperate by withholding information on tax-relevant matters or providing false information, the tax authorities have virtually no way of assessing foreign taxable income in accordance

226 Fiscal Code Application Decree (Anwendungserlass zur Abgabenordnung, AEAO of 2014) of 31 January 2014, last amended by BMF letter of 19 June 2018, VV DEU BMF 2018-06-19 IV A 4-S 0316/13/10005:053.

227 Kraft/Ditz/Heider, "Internationaler Informationsaustausch", DB 2017, 2243.

228 See Czakert, "Die gesetzliche Umsetzung des Common Reporting Standards in Deutschland", DStR 2015, 2697.

with the provisions of substantive law. Apart from these cases of criminal conduct, the knowledge asymmetry between highly professional tax advisers with international operations on the one hand and the tax authorities on the other also has a negative impact on the balance and fairness of the tax system. The lack of coordination between tax law systems provides ample tax planning opportunities for separating the place of profit generation from that of taxation. It is not illegal to take advantage of these types of planning opportunities – on the contrary, such course of action is a protected fundamental right, because it gives taxpayers the opportunity to minimise their companies' tax burden within the limits allowed by tax law.[229] However, aggressive tax avoidance strategies result not only in under-collection of tax, but also distort the competitive environment. This affects small and medium-sized companies that operate exclusively in domestic markets or are unable to develop similar tax avoidance strategies because of the associated transaction costs.[230] A salient example that dramatically brought home the extent of the problem is the Luxembourg leaks, confirming the need and justification for the BEPS action plan.[231]

Triggered by measures to counter tax evasion taken in the United States, and above all as part of the BEPS project, a dense network of legal foundations has been woven at both international and European level, and this has taken the international exchange of information to new heights in terms of both quantity and quality. Intergovernmental cooperation among tax authorities has taken on a different quality, especially as a result of the expanded automatic exchange of information. Unlike the exchange of information on request – where one country requests from another information it needs to make its own tax assessment – and the spontaneous exchange of information – where information is transferred without prior request, because it is expected to be tax-relevant in the other country – the automatic exchange of information involves transferring information to another country systematically and regularly without the need for a specific request.[232] The overview below will be limited to covering the development and expansion of the automatic exchange of information.

bb) Overview of the legal foundations of automatic exchange of information

An overview of the reach of the automatic exchange of information is hampered by the coexistence of the different legal foundations, which fall within the jurisdictions of international, EU and national law.[233] The basic standard for the international exchange of information in national law is section 117 of the AO. Subsection 1 governs the use of international legal and administrative assistance by German tax authorities. It specifies that the tax authorities may avail themselves of international legal and admin-

229 Stöber, "Anzeigepflichten in Bezug auf Steuergestaltungen im deutschen und europäischen Recht", BB 2018, 1559.

230 OECD (fn. 52), p. 8 f.; see recital 2 to Directive 2016/881/EU (fn. 249).

231 BT-Drs. 18/5776, p. 1 f.

232 Oppel, "Internationaler Informationsaustausch in Steuersachen – Teil "I, NWB, 359 (361); see Czakert (fn. 229) (2698).

233 See e.g. Hamacher, "Datenschutz und internationaler Informationsaustausch", IStR 2016, 171.

istrative assistance subject to the provisions of German law Since international legal and administrative assistance is a sub-category of administrative assistance, the requirements of sections 111 ff. of the AO must be met, specifically the criterion that administrative assistance must be necessary (section 111 f. of the AO).[234] In contrast, section 117 (2)-(4) of the AO governs international legal and administrative assistance in the opposite direction, i.e. it deals with the question of whether and to what extent German tax authorities are required to provide legal and administrative assistance.[235] Pursuant to these provisions, the tax authorities may provide international legal and administrative assistance on the basis of nationally applicable international agreements, nationally applicable legal instruments of the European Union and the EU Mutual Assistance Act. Contrary to its wording ("may"), section 117 (2) of the AO constitutes an obligation to provide legal and administrative assistance, providing that the factual requirements under the applicable legal norms are met.[236]

(1) Savings Directive and Directive 2011/16/EU – DAC 1.

In the European Union, the automatic exchange of information was implemented as early as in 2003 on the basis of the EU Savings Directive, which has since been repealed.[237] The directive governed the automatic provision of information on savings income by the Member State collecting the interest to the Member State receiving it. In 2011, the Directive on administrative cooperation in the field of taxation (2011/16/EU) entered into force (Directive on Administrative Cooperation – DAC 1),[238] replacing the previous Mutual Assistance Directive[239]. The Directive on Administrative Cooperation of 2011 has since been expanded in several stages (DAC 2, DAC 3, DAC 4, DAC 5 and most recently DAC 6). The Directive on Administrative Cooperation (DAC 1) already provided for the automatic exchange of information on certain types of income, including supervisory board and administrative board remuneration as well as ownership of immovable property and income from such property (Art. 8(1)(b) and (e) DAC 1).

(2) Directive 2014/10/EU – DAC 2.

Further expansion of the automatic exchange of information was subsequently triggered by US tax legislation: on the basis of the Foreign Account Tax Compliance Act, foreign financial institutions in

234 For more on this and the discretionary limits of proportionality and reasonableness on using international legal and administrative assistance, see Seer, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, 2016, section 117 marginal note 24 f.

235 Seer, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, 2016, section 117 marginal note 8.

236 Seer, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, 2016, section 117 marginal note 69.

237 Council Directive 2003/48/EC of 3 June 2003 on taxation of savings income in the form of interest payments, OJ EU L 157/38 of 26 June 2003.

238 Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (OJ EU L 64/1 of 11 March 2011).

239 Council Directive of 19 December 1977 concerning mutual assistance by Member States in the field of direct taxation (77/799/EEC – OJ EC No L 336/15 of 27 December 1977).

the USA have been required since 2010 to provide account information on account holders who are subject to tax in the USA.[240] In order to clarify data protection issues and ensure reciprocity, Germany and other EU Member States initially entered into agreements with the USA based on the OECD Model Convention. On the basis of these agreements, the OECD was requested to prepare a uniform global standard for automatic exchange of tax information. In September 2014, this standard was approved by the finance ministers and central bank governors of the G20 (Common Reporting Standard, CRS[241]).[242] At the European level, this standard was implemented by way of Amending Directive 2014/10/EU (DAC 2),[243] which also repealed the Savings Directive, which it had superseded. German legislators implemented the requirements of the directive in the German Financial Accounts Information Exchange Act (Finanzkonten-Informationsaustauschgesetz, FKAustG)[244]. The CRS has its basis in international law in the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (MCAA 1) entered into as at 29 October 2014 on the basis of Art. 6 of the multilateral European law/ OECD convention.[245]

(3) Directive 2015/2376/EU – DAC 3.

Directive 2015/2376/EU (DAC 3), which governs mandatory automatic exchange of advance cross-border rulings and advance pricing arrangements (Art. 8a and 8b DAC), marks another step in the expansion of automatic exchange of information.[246] Even though the recitals do not mention this specifically, in terms of legal policy the directive was a response to the Luxembourg leaks, which exposed the practice of the Luxembourg tax authorities: they had allowed multinational companies, under the protection of Luxembourg's advance tax rulings, to shift considerable amounts of income to the domestic territory, where it was subject to lower taxation – to the detriment of other Member States.[247]

---

240 Ruiner/Schramm/Fischer, "Foreign Account Tax Compliance Act", DB 2011, 2403 ff.

241 See OECD, Standard for automatic exchange of financial account information in tax matters, 2nd ed. 2017.

242 Recitals 2-4 to Directive 2014/107/EU (fn. 244).

243 Council Directive 2014/107/EU of 9 December 2014 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation; for an instructive overview, see Seer, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, 2016, section 117 marginal note 56.

244 Gesetz zum automatischen Austausch von Informationen über Finanzkonten in Steuersachen (Finanzkonten-Informationsaustauschgesetz, FKAustG (German Financial Accounts Information Exchange Act)) of 21 December 2015 (BGBl. I p. 2531).

245 For a representative example, see Seer, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, 2016, section 117 marginal note 53.

246 Council Directive (EU) 2015/2376 of 8 December 2015 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation (OJ EU L 332/1 of 18 December 2015).

247 Recital 1 to Directive 2015/2376/EU (fn. 247).

(4) Directive 2016/881/EU – DAC 4.

Directive 2016/881/EU (DAC 4)[248] requires multinational groups with revenue above a threshold of €750 million to disclose to the tax authorities, on an annual basis for all tax jurisdictions in which they operate, information such as the amount of revenue, pre-tax profit or loss, tax paid and accrued, the number of employees, stated capital, accumulated earnings and tangible assets in each tax jurisdiction (Art. 8aa DAC 4). By means of an automatic exchange, the competent authority of the Member State of the group parent has to communicate the country-by-country reports to any other Member State in which one or more entities of the multinational group are resident for tax purposes or subject to tax based on the business carried out from a permanent establishment (Art. 8aa(2) DAC 4). The directive was transposed into German tax procedure law by way of section 138a of the AO.[249] The legal policy basis of this new variant of the automatic exchange of information is the OECD/BEPS action plan presented back in July 2013.[250] Action 13 specifies the preparation of transfer pricing documentation to enhance transparency for tax administrations, taking into consideration the compliance costs for business. As an element of the guidance still to be developed, the prospect was raised of an obligation on companies with global operations to provide all relevant countries with the information required on how the companies' income, economic activities and taxes paid break down to the different countries around the world.[251] At the OECD level, this was implemented in the final report on "Transfer Pricing Documentation and Country-by-Country Reporting" on 5 October 2015.[252] This report sets out a three-stage approach, revising the existing OECD standards for transfer pricing documentation. According to this approach, multinational companies are required to submit to the tax authorities a master file with fundamental information on their global business activities and transfer pricing policies. A local file, which has to be prepared separately for each country, has to contain information on all material transactions with associated third parties and an analysis of the transfer pricing regulations. The first two stages were based on the code of conduct on transfer pricing documentation for related enterprises in the European Union and on existing practice. However, the third element (country-by-country report) enters uncharted territory, which is described as follows in the final report:

> According to this report, "large MNEs [multinational enterprises] are required to file a Country-by-Country Report that will provide annually and for each tax jurisdiction in which they do business the amount of revenue , profit before income tax and income tax paid and accrued.

248 Council Directive (EU) 2016/881 of 25 May 2016 amending Directive 2011/16/EU as regards the mandatory automatic exchange of information in the field of taxation.

249 Gesetz zur Umsetzung der Änderungen der EU-Amtshilferichtlinie und von weiteren Maßnahmen gegen Gewinnkürzungen und -verlagerungen (German Act Implementing the EU Directive on Administrative Cooperation and Other Actions against Base Erosion and Profit Shifting) of 20 December 2016 (BGBl. I p. 3000).

250 OECD (fn. 52).

251 OECD (fn. 52); more detail: OECD, Transfer pricing documentation and country-by-country reporting, 2015.

252 OECD (fn. 252).

> It also requires MNEs to report their number of employees, stated capital, retained earnings and tangible assets in each tax jurisdiction. Finally, it requires MNEs to identify each entity within the group doing business in a particular tax jurisdiction and to provide an indication of the business activities each entity engages in."[253]

In addition to its implementation at EU level in Directive 2016/881/EU, Action 13 of the BEPS project has become binding in international law by way of another Multilateral Competent Authority Agreement[254], to which 71 countries have become signatories in addition to Germany.

(5) Directive 2016/2258/EU – DAC 5.

Directive 2016/2258/EU (DAC 5)[255] requires Member States as from 1 January 2018 to allow their tax authorities access to data relating to beneficial owners. The intention is to make it easier for these tax authorities to meet their obligations under the Directive on Administrative Cooperation (Directive 2011/16/EU) and combat tax evasion and fraud more effectively.[256] In Germany, this requirement was already implemented in section 23 (1) letter e of the GwG, so that no further amendments are needed.

(6) Directive 2018/822/EU – DAC 6.

The most recent amendments to the Directive on Administrative Cooperation are dated 5 June 2018. Directive 2018/822/EU (DAC 6)[257] is intended to make it mandatory for intermediaries or taxpayers to report potentially aggressive tax planning to the national authorities. The directive must be adopted by 31 December 2019 and its provisions must be applied as from 1 July 2020 (Art. 2(1) Directive 2018/822/EU). The directive does not amend the right as such to choose tax planning opportunities that take advantage of loopholes in tax laws or result from the lack of coordination between tax law systems. However, the provision of information on aggressive tax planning to the Member States is intended to enable them to react promptly against harmful tax practices and to close loopholes by enacting legislation or by undertaking adequate risk assessments and carrying out tax audits. In addition, the reporting requirement is intended to act as a deterrent.[258] The information will, once again, have to be provided by means of an automatic exchange (Art. 8ab(13) Directive 2011/16/EU, new version).

---

253 OECD, Transfer Pricing Documentation and Country-by-Country Reporting, Action 13 - 2015 Final Report, 2016.

254 Seer, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, 2016, section 117.

255 Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities (OJ EU L 332/1 of 16 December 2016).

256 Recital 4 to Directive (EU) 2016/2258 (fn. 256 above).

257 Council Directive (EU) 2018/822 of 25 May 2018 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements (OJ EU L 139/1 of 5 June 2018).

258 See recital 4 to Directive (EU) 2018/822 (fn. 258 above).

The information to be communicated is specified in detail in Art. 8ab(14) Directive 2011/16/EU, new version. Of particular relevance in this context are the name, date and place of birth and the value of the reportable cross-border arrangement (Art. 8ab(14)(a)(f) Directive 2011/16/EU, new version). The fact that a Member State does not react to such a report does not imply any acceptance of its validity. The directive expressly forbids this reverse conclusion (Art. 8ab(15) Directive 2011/16/EU, new version).

The Conference of the Ministers of Finance of the federal state governments intends to implement the directive with additional requirements in Germany by making the reporting requirement applicable to national tax planning as well.[259] The provisions of the directive are not entirely unprecedented: in 2007, the BMF had submitted a similar proposal in a draft section 138a of the AO, although it never became law.[260] Similar requirements have been in place in the United Kingdom since 2004 and are also governed by current US law.[261] The directive was once again triggered directly by the BEPS action plan, whose action 12 requires "taxpayers to disclose their aggressive tax planning arrangements".[262] The publication of the Panama Papers and the Paradise Papers is expected to provide support for this project.[263] The legal policy intention underlying the disclosure requirement certainly seems reasonable because the beneficiaries of aggressive tax planning create advantages over their competitors that seem unjustified and counter to the idea of distributing the tax burden fairly. The weak point of the directive is probably the fact that its substantive scope has not been defined with sufficient clarity. On this point, the directive refers to cross-border tax planning arrangements, which correspond to hallmarks itemised in a list in Annex IV to the directive. It remains to be seen whether this list will be able to meet the expectations placed on it. The issue is expected to keep advisory practice, tax administration and tax litigation extremely busy with questions relating to the legal force of the disclosure requirement.

3. Public country-by-country reporting

From a data protection perspective, the measures outlined above are far from unproblematic because they involve the exchange of sensitive personal data in some cases, which will be included in a data pool and may therefore potentially be misused. A cause for concern in this regard is, for example, a

259 See https://fm.rlp.de/de/presse/detail/news/detail/News/gesetzentwurf-zur-anzeigepflicht-fuer-nationale-steuergestaltungsmodelle-gebilligt/

260 See http://www.gmbhr.de/heft/15_07/StGestAnzPflG_RefEntw.pdf; critical opinion on the proposal submitted at the time: Schenke, *Verfassungs- und europarechtliche Fragen des § 138a AO-Entwurf*, August 2007 (legal opinion: available at Lexinform 0208905).

261 Schnitger/Brink/Welling, "Die neue Meldepflicht für grenzüberschreitende Steuergestaltungen (Teil I)", IStR 2018, 513.

262 OECD (fn. 52), p. 27.

263 See website of the PANA Committee established by the European Parliament (http://www.europarl.europa.eu/committees/de/pana/home.html).

decline in efforts in some Member States to take decisive action against corruption.[264] Nevertheless, the invasions of privacy associated with the amendments to the Directive on Administrative Cooperation (2011/16/EU) fall outside the scope of investigation of this study because, to date, the directive does not set out any disclosure requirements, i.e. unlike the transparency register the data is not entered in a publicly accessible register.

This would change if the European Commission's proposal were to prevail: it wants to subject the country-by-country report, which has so far only been communicated to other affected countries, to a general disclosure requirement. The corresponding initiative dates back to April 2016.[265] The proposal is not based on the tax law harmonisation powers of Art. 115 and Art. 114(2) TFEU, but the harmonisation powers intended to attain freedom of establishment pursuant to Art. 50 TFEU. In the European Commission's opinion, this has the strategic advantage that Art. 50 TFEU does not specify the consensus requirement that applies to tax law harmonisation. It is therefore proposing that the provisions should be added to the Directive on Annual Financial Statements rather than the Directive on Administrative Cooperation.[266]

This approach is prone to draw considerable objections in relation to the division of powers. The recitals to the directive clearly focus on the tax law aspect. They read as follows:

> "Fighting against tax avoidance and aggressive tax planning, both at EU and global level, is a political priority for the European Commission. As part of a broader strategy for a Fair and Efficient Corporate Tax System in the EU, public scrutiny can help to ensure that profits are effectively taxed where they are generated. Public scrutiny can reinforce public trust and strengthen companies' corporate social responsibility by contributing to the welfare through paying taxes in the country where they are active. In addition, it can also promote a better informed debate on potential shortcomings in tax laws."[267]

---

264 See WELT of 22 July 2018 (https://www.welt.de/politik/ausland/article178581732/Rechtsstaat-Ungarn-Polen-So-hebelt-Rumaenien-gerade-die-Justiz-aus.html).

265 Proposal for a Directive of the European Parliament and of the Council amending Directive 2013/34/EU as regards disclosure of income tax information by certain undertakings and branches.

266 Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ. EU L 182/19 of 29 June 2013).

267 Proposal (fn. 266), p. 2.

The actual recitals point in the same direction. The introduction reads as follows:

> "In recent years, the challenge posed by corporate income tax avoidance has increased considerably and has become a major focus of concern within the Union and globally. The European Council in its conclusions of 18 December 2014 acknowledged the urgent need to advance efforts in the fight against tax avoidance both at global and Union level. The Commission in its communications entitled 'Commission Work Programme 2016 - No time for business as usual' and 'Commission Work Programme 2015 - A New Start' identified as a priority the need to move to a system whereby the country in which profits are generated is also the country of taxation. The Commission also identified as a priority the need to respond to our societies' call for fairness and tax transparency."[268]

There is therefore a convincing argument for assuming that the directive should rightly be based exclusively on tax law harmonisation powers rather than Art. 50 TFEU. The proposed directive is obviously aimed at strengthening tax compliance, meaning that its emphasis must be on tax law. In addition to the rationale and the political context, procedural considerations also suggest this. As evidence that the proposal is not intended to add to the bureaucratic burden in any significant way, the European Commission points out that large multinational enterprises have to submit extensive country-by-country reports to the tax authorities in any case. However, since there is an uncontested view that this has its basis in tax law, it is simply inconceivable that the matter could be taken out of its tax law context merely by introducing a requirement to publish the data. Disclosure requirements have an instrumental significance, even in the context of the requirement to publish annual financial statements. To avoid a scenario where the division of powers, whose function is to protect the (tax law) sovereignty of the Member States, is put at the free disposal of the European Commission, a disclosure requirement cannot be allowed to have an effect on the ability to determine harmonisation powers.

In addition to objections relating to the division of powers, the proposal also has shortcomings in terms of data protection. Given the severity of the invasion associated with the disclosure requirement, it is surprising to see so few explanations – barely enough to demonstrate that the Commission is aware of the problem. The recitals to the proposed directive merely state in this regard:

> "This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union."[269]

---

268 Recital 1 (fn. 266).

269 Recital 15 (fn. 266).

The section on the results of the ex-post evaluation, the consultation of interested parties and the evaluation of potential consequences hardly adds anything of substance to the considerations:

> **"Fundamental rights**
> Overall, the extent of information envisaged is proportionate to the objectives of enhancing public transparency and scrutiny. Reporting builds on information generally published in financial statements of most of MNE groups in the EU."[270]

Objectively, the disclosure requirement is based on BEPS action 13, meaning that only multinational groups with consolidated revenue of more than €750 million are to be required to submit a country-by-country report.[271] The contents to be disclosed relate to the nature of the activities, the number of persons employed, the net turnover made (including with related parties), the profit made before tax, the amount of income tax due in the country owing to the profit made in the current year, the actual payments made to the country's treasury during that year and the amount of accumulated earnings.[272] The recitals do not make reference to any significant difference between the proposed directive and the BEPS action plan, which does not recommend any disclosure requirement at all, meaning that the proposed directive has overreaching tendencies and significantly exceeds what the community of nations had agreed.

The consolidated income tax information report is primarily intended for publication in the business register. In addition, however, the reports are to be made available on the companies' websites, where they have to be accessible for at least five years in succession.[273]

It is difficult to predict at present whether the European Commission's proposal for a directive has any prospect of being realised, after the consultation process stalled following, among other things, Parliament's opinion at the first reading stage, with discussions in the Council and its preparatory official positions, on 19 December 2017.[274]

IV. Holistic view

Whether the disclosure requirements discussed above interfere with the right to informational self-determination (see section D for details) to an unreasonable extent is impossible to assess by looking at

270 Proposal (fn. 266), p. 6.

271 Proposal (fn. 266), p. 7.

272 Proposal (fn. 266), p. 8.

273 Proposal (fn. 266), p. 9.

274 For information on the status of the initiative, see https://eur-lex.europa.eu/procedure/EN/2016_107.

the provisions in isolation. Instead, we have to consider all publicly accessible information as a whole, because the risks of modern information technology, which data protection seeks to counter, come to bear when data that may seem unproblematic when viewed in isolation is analysed as a combined whole.

Consider the situation of a student, for example, who has two siblings and, as a result of intestate succession after the death of her parents, holds more than 25 per cent of the parents' business: through various publicly accessible sources of information, her financial status can be relatively reliably determined. Being a "beneficial owner", her first and last name, date of birth and place of residence will appear in the transparency register (section 19 (1) of the GwG). The register will also reveal the nature and extent of the beneficial interest she holds. If the company is subject to the rules on publishing annual financial statements – which most companies are – analysis of the statements can produce an estimate of the financial value of the equity investment. If the company is a stock corporation, it is even possible to look up the company founder's private address in the commercial register, and the heiress may still live at this address.

This additional dimension of public data accessibility is attributable in particular to the transparency register, which intentionally seeks to break through the façade of the legal person to identify the natural persons behind it. There may be a valid need for this kind of access in cases of money laundering and terrorism financing. However, the transparency register indiscriminately captures all persons who hold interests in a company. The magnitude becomes clear when you consider the number of corporations in Germany: the country has more than one million GmbHs and stock corporations. Since an interest of more than 25 per cent is deemed enough to demonstrate beneficial ownership, the reporting requirement is expected to affect many millions of citizens, the vast majority of whom have never come into contact with money laundering or terrorism financing. And after the implementation of MLD 2018, access to this information will by no means be restricted to authorities responsible for criminal prosecution, but anyone in the entire territory of the European Union – and worldwide in fact, since internet-based databases can be accessed across national borders.

In pragmatic terms, the fact that the relevant registers cannot be searched for individuals, at least in Germany, provides some measure of protection. In both the commercial register and the transparency register, the search request must relate to a specific company. Although searches for individuals are not possible, if you know the name of the company, an individual search is no longer a barrier, and you can proceed to identify the beneficial owners. What is more, this purely logistical hurdle to determining information is merely a relic of the outdated structure of the German register management system. Modern technology would permit much more efficient search methods. There are no legal precautions in the applicable laws that prevent the modernisation of the registers in this direction. The commercial registers of other EU Member States are already much more efficient – from the perspective of the user submitting search requests. This is similarly expected to apply to the transparency registers.

MLD 2018 only contains limited provisions to prevent data misuse or protect the data from use for anything other than the original purpose. In exceptional circumstances, Member States "may provide for" an exemption for minors or otherwise legally incapable persons (Art. 30(9) MLD 2018). Individuals who are not minors are not granted any special protection. Moreover, this is only an option that can be laid down in national law. If there are individual Member States that do not exercise this option, shareholders who are minors and potentially benefit from the exemptions in their home countries will nevertheless be included in the transparency registers of other countries, which can be accessed by anyone worldwide. Such a scenario could easily occur if the parents' company has a foreign subsidiary in a country where legislators have not exercised the option of allowing an exemption.

In addition, Art. 30(9) MLD 2018 permits an exemption if the beneficial owner would be exposed to disproportionate risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation. This exemption would also have to be laid down specifically in national law, and this course of action may not be pursued by all Member States; it would therefore not provide reliable protection for companies with international operations. If you consider, for example, the current version of section 23 (2) of the GwG, which already provides for such an exemption, it becomes clear, moreover, that this protection from crime is in fact ineffective: the individual concerned has to disclose facts that "justify the assumption that access to the information would expose the beneficial owner to the risk of falling victim to one of the following crimes: (…)". If there is evidence that there is a risk of crime (e.g. threatening letters or phone calls), the potential criminal already has the individual concerned in his or her sights. The exemption is thus rendered largely ineffective, since the requirements for it to apply can only be met if the risk to be avoided has already occurred.

Lastly, reference should be made to the sometimes inappropriate use of this kind of data by the media and social networks; in the area of board remuneration, there is already material that can illustrate such behaviour (see C.II.1.e)dd above). If, in addition to the transparency register, country-by-country reporting were also made accessible to anyone, headlines such as "millionaire heiress involved in tax scandal" will not be far behind. The fact that, legally and factually, a student holding a little more than 25 per cent of a company is normally unable to exert any meaningful influence on the company's tax planning is likely to be ignored in this kind of debate, as is the question of whether the tax planning was actually unlawful or merely advantageous. It is in fact virtually impossible to fight back against such attacks. An attempt to do so would draw even more attention without really convincing the average consumer of such information. For this reason, legislators should seriously consider whether it is really necessary to put an individual's personal integrity at risk in this way in order to achieve the legal policy objectives of the provisions in question.

D. Assessment under EU and constitutional law

I. Basic principles

As shown above, the latest expansion of company-related disclosure requirements, which has already been implemented or is undergoing the legislative process, is entirely based on European requirements. This is of importance for the interpretation of the national implementing acts as well as for the fundamental rights standards applicable to them.

Since EU law takes precedence, Germany's Basic Law, in particular the test function of German fundamental rights, is relegated to a secondary position behind EU law.[275] According to ECJ case law, this means that the fact that a directive, or even a national implementing act, is in conflict with the fundamental rights provided for in the Basic Law cannot be used as an argument against the directive or national implementing act.[276] The restrictions formulated by the Federal Constitutional Court in this regard only have theoretical significance in this context.[277] Although the Federal Constitutional Court safeguards the substance of German fundamental rights, including vis-à-vis EU legislators[278], in its recent judgements the ECJ has, however, developed even stricter data protection requirements than those demanded by the BVerfG, meaning that the protection of fundamental rights at the European level is at least equal. This point will be covered in more detail below. Following tighter protection of fundamental rights in Europe, especially in the area of data protection, there is no expectation that the Federal Constitutional Court's reservation will attain practical significance in the foreseeable future.

This means that the only room that remains for applying national fundamental rights standards is determined by the extent to which EU law gives the National States flexibility for implementation, which will then have to be utilised in accordance with the values set out by national constitutional law. In contrast, the effectiveness of secondary law only has to stand up to measurement against European fundamental rights standards,[279] in the same way as secondary law – and the national law that defines it – has to be clarified in accordance with European fundamental rights standards.[280] Nevertheless, the judgements of

---

275 Similar conclusion in Wartenburger, in: Schön, *Rechnungslegung und Wettbewerbsschutz im deutschen und europäischen Recht*, 2009, p. 49 (54 ff.).

276 Settled case law since ECJ judgement of 15 July 1964 – C-6/64 (Costa / ENEL), Sammlung Beck 1964, 1251 (1269 ff.).

277 General information on the interplay between national and European fundamental rights protection, see Ludwigs, "Kooperativer Grundrechtsschutz zwischen EuGH, BVerfG und EGMR", EuGRZ 2014, 273.

278 BVerfGE 73, 339 ff.

279 BGHZ 208, 82 marginal note 33.

280 For Charter-compliant interpretation of directives, see e.g. ECJ judgement of 9 March 2017, C-398/15 (Salvatore Manni), ECLI:EU:C:2017:197 marginal note 39; ECJ judgement of 6 October 2015, C-362/14 (Schrems), ECLI:EU:C:2015:650 marginal note 38.

the Federal Constitutional Court also attain lasting significance: since the BVerfG developed the fundamental right to informational self-determination in the census ruling handed down at the end of 1983, a detailed system of finely worded authoritative writing has been captured in a comprehensive collection of case law extending to 81 subsequent volumes. This is why BVerfG case law serves as a repository of problem solutions and a source of inspiration for enhancing the protection of fundamental rights at the European level even in areas where the Basic Law no longer applies directly. In terms of primary law, this is recognised in Art. 6(3) TEU, which states that the fundamental rights, as they result from the constitutional traditions common to the Member States, constitute general principles of the Union's law. Without attempting to advocate German "fundamental rights imperialism", the case law of the Federal Constitutional Court in Karlsruhe should at least be respected as a source of fundamental legal principle.

Nevertheless, since the Treaty of Lisbon entered into force, the Charter of Fundamental Rights has been at the centre of European protection of fundamental rights (Art. 6(1) TEU). Art. 7 CFREU guarantees respect for private and family life and Art. 8 CFREU the protection of personal data. In addition, however, fundamental rights, as 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, must also be respected as general principles of the Union's law (Art. 6(3) TEU). This manifests itself above all in Art. 8 ECHR, which guarantees respect not only for one's family life, home and correspondence, but also for one's private life. In European data protection law, special attention should therefore be paid to the judgements of the ECtHR, given that they have influenced the data protection provisions of the Charter to a significant extent as evidenced by the explanations to the Convention.[281] At the level of secondary law, these control standards under primary and international law are complemented by the Data Protection Directive.

II. Control standards

In the hierarchy of norms, the CFREU and the Data Protection Directive take priority over other control standards.[282] The discussion below deliberately opts not to follow the sequence determined by the hierarchy of norms so it can present the interaction between control standards in the Union as they have have evolved historically.

1. Fundamental right to informational self-determination (article 2 (1) in conjunction with article 1 (1) of the GG)

The fundamental right to informational self-determination was created by way of the BVerfG's census ruling handed down in 1983.[283] As explained above, in matters governed by EU law, the fundamental

281 See Explanations relating to the Charter of Fundamental Rights (2007/C 303/02), p. 20.

282 See p. 73 above.

283 BVerfGE 65, 1 (43 ff.).

right to informational self-determination is relegated to a secondary position behind EU protection of fundamental rights. However, it continues to be relevant even in matters governed by EU law, if German legislators decide to regulate over and above the disclosure requirements resulting from mandatory European provisions.[284] What is more, the rulings of the Federal Constitutional Court in Karlsruhe have had a considerable influence on the development of European fundamental rights protection.

The fundamental right to informational self-determination is a subset of the general right of personality laid down in article 2 (1) in conjunction with article 1 (1) of the GG.[285] The general right of personality guarantees each individual an autonomous sphere of private life in which to develop and safeguard his or her individuality.[286] As a subset of this right, the fundamental right to informational self-determination guarantees each individual the right to determine how his or her personal data may be collected and used. Especially under the conditions of electronic data processing, which allows the almost unlimited recording, reproduction and combination of personal data, informational self-determination thus serves to safeguard the fundamental right to practice individual freedom.

Case law justifies the special sensitivity with reference to the intimidating effect, i.e. the theory that knowledge about an observation, registration and recording of personal circumstances may lead to a change in behaviour.[287] One example of evasive action that could be taken in response to the transparency register is a plan to restructure companies in order to circumvent the disclosure requirement. The only option that remains for affected individuals who want to avoid the public limelight is to refrain from ever acquiring an interest of more than 25 per cent in any company, irrespective of size.

Depending on the method used to collect information, the provisions of article 2 (1) in conjunction with article 1 (1) of the GG are superseded by special fundamental rights, such as article 10 of the GG for telecommunications surveillance and article 13 of the GG for private home surveillance. Since there is a recognisable trend to interpret the different fundamental rights for the protection of privacy in the same way, the exact definition of each area of protection only has relative importance, so that it does not have to be considered any further in the present context.[288]

---

284 An example of this kind of approach is France, which has introduced public country-by-country reporting, thus exceeding the requirements of the directive.

285 Many possible examples of how to classify the fundamental right, represented here by Di Fabio, in: Maunz/Dürig, *Grundgesetz*, 2013, article 2 (1), marginal note. 173.

286 BVerfGE 79, 256 (268); 117, 202 (225).

287 See BVerfGE 100, 313 (381); 109, 279 (354); BVerfGE 9, 62 (77); BVerfGE 120, 274 (323); 120, 378 (402, 430); see Di Fabio, in: Maunz/Dürig, *Grundgesetz*, 2013, article 2 (1) marginal note 175, including on informational self-determination as a guarantee of the individual's freedom to make decisions.

288 For views on the convergence of fundamental rights dogmatism for the protection of privacy and on opposite trends, see Schenke, in: Stern/Becker, *Grundrechtskommentar*, article 10 marginal note 45.

Personal data is data on the personal or factual circumstances of identifiable individuals.[289] This also includes tax data in particular.[290] Since modern information technology allows the combination of seemingly insignificant data, which can be consolidated into a comprehensive personal profile, protection is granted irrespective of the quality and informative value of the data collected.[291] The fundamental rights provide protection not only at the time the data is initially collected, but also for any subsequent use of the data, meaning that each change of purpose is deemed a new intervention. This also includes the communication of such data to other public and non-public entities, because this extends the group of persons who can look at and use the data.[292] If public authorities grant access to the personal data of third parties, it is therefore considered interference with the right to informational self-determination.[293] The protection also extends to data that is in the public domain or generally accessible.[294]

The fundamental right is not granted completely without limitations; instead, it is subject to a general legal reservation. Being a special subset of the principle of legal certainty and the fundamental law principle of legal reservation, interference with informational self-determination requires clear legal arrangements that apply to a specific area.[295] This means that the interference must be clearly set out in law. This forces legislators to accept the political responsibility for interfering with fundamental rights and to subject the need for such interference to interrogation during the parliamentary process and the ensuing debate in the critical public. This gives advance warning to citizens of any interference, which can then be subjected to effective control by the courts.

The physical barrier of interference with the right to informational self-determination is the principle of proportionality. Based on this principle, the BVerfG has developed a large number of demands against which interference with informational self-determination can be measured. This includes special requirements for the protection of fundamental rights through organisation and procedures, including effective legal protection and the need for rules on data deletion.[296] Since the BVerfG has granted legislators scope for assessing and weighing up alternatives, the principle of interference with informational self-determination will not normally be called into question. Instead, the BVerfG has limited its activities

289 Jarass, in: Jarass/Pieroth, GG, 14th ed. 2016, article 2 marginal note 43.

290 BVerfGE 67, 100 (142 f.).

291 Di Fabio, in: Maunz/Dürig, *Grundgesetz*, 2013, article 2 (1), marginal note. 174.

292 Schoch (fn. 40), section 5 marginal note 8 f.

293 Schoch (fn. 40), section 5 marginal note 9.

294 BVerfGE 120, 351 (361); 120, 378 (399).

295 Most recently BVerfGE 141, 220 marginal note 94.

296 For information on the need for protection requirements under procedural law, see Di Fabio, in: Maunz/Dürig, *Grundgesetz*, 2013, article 2 (1), marginal note 178.

to expanding data protection safeguards. An example is the Federal Constitutional Court's ruling on data retention, which – unlike the judgement of the ECJ[297] – did not categorically reject this investigative technique, but merely imposed limits on it in accordance with the rule of law.

2. Right to respect for private life (Art. 8 ECHR)

Art. 8(1) ECHR guarantees each individual's right to respect for his or her private and family life, home and correspondence. Even if, in derogation of Art. 6(2) TEU, the European Union has not adopted the ECHR,[298] the level of data protection set out in Art. 8 ECHR is at least an indirect touchstone for EU law. Art. 6(3) TEU incorporates the fundamental rights guaranteed in the ECHR as general principles into EU law. Furthermore, the fundamental rights in the Charter that correspond to those in the ECHR have the same significance and reach in the ECHR (Art. 52(3)(1) CFREU), unless European Union law provides further-reaching protection. The concept of a minimum level of protection is finally also addressed in European secondary and data protection law.[299]

Art. 8 ECHR provides protection for a sphere of the individual in which people can live according to their beliefs and strive to fulfil and develop their personalities, thus enabling them to develop physically and mentally.[300] Data protection is an important sub-element of the right to respect for private life. This seems logical, since the collection, storage and use of personal data has considerable potential to interfere with the right to realise one's potential, which follows on from the protection of private life.[301] Similar to the BVerfG's reasoning, the intimidation theory is likely to be the underlying driver.[302]

Similar to the fundamental right to informational self-determination, the right to respect for private life does not come with a limitless guarantee. Art. 8(2) ECHR lays down a legal reservation and specifies that any law that limits rights has to meet one of the objectives listed there. The list of purposes includes national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. However,

297 See D.IV.1.d) below (p. 88).

298 ECJ, opinion of 18 December 2014, C-2/13 (signature and ratification of ECHR), ECLI:EU:C:2014:2454.

299 See recital 10 to Directive 1993/46/EC.

300 ECHR of 11 July 1980 – 8307/78 – Deklerck/Belgium; Grabenwarter/Pabel, *EMRK*, 5th ed. 2012, section 22 marginal note 6; Meyer-Ladewig/Nettesheim, in: Meyer-Ladewig/Nettesheim/von Raumer, *EMRK*, 2017, Art. 8 marginal note 7.

301 Gersdorf, in: BeckOK, *Informations- und Medienrecht*, 20th edition, Art. 8 ECHR marginal note 29.

302 See ECtHR, NJW 1979, 1755 (1756) – Klass/Germany on freedom of communication; ECtHR, NJW 2004, 3317 (3319) – Steur/Netherlands, where it is translated as "restraining effect". See ECtHR, application no. 33348/96 – Cumpana and Mazara/Romania.

legislators may only invoke one of these purposes if the interference is necessary in a democratic society. This criterion is the starting point of a proportionality test.[303]

In principle, the ECtHR gives Member States considerable scope for balancing competing interests in the area of private life. The backdrop to this approach is probably that opinions on how far the protection of private life should reach are very divergent between Member States, so the imposition of standards formulated through court rulings must also seem problematic from a democratic perspective.[304] The ECtHR attaches unusually high importance to data protection, however. This is evidenced, for example, by the fact that it does not give carte blanche to impose restrictions, even for purposes of criminal prosecution.[305]

3. Data Protection Directive 1995/46/EC

A milestone in the development of European data protection law is the Data Protection Directive 95/46/EC adopted in October 1995.[306] The directive has since been superseded by the General Data Protection Regulation (Art. 94(1) GDPR); references to the repealed directive are construed as references to the GDPR (Art. 94(2) GDPR). Nevertheless, the directive continues to be of importance. Since the European Convention made reference to the directive when determining the level of data protection as a fundamental right in the CFREU,[307] the directive remains an important aid in interpreting Art. 8 CFREU (protection of personal data). In addition, the GDPR's basic concept is largely based on the Data Protection Directive 1995/46/EC.[308]

The Data Protection Directive pursued a dual aim. The recitals emphasise that the realisation of the objective of the Single Market requires exchanges of personal data, although this is hampered by different levels of data protection in the Member States.[309] To remove the obstacles to the communication of personal data, the directive therefore aims at equivalent levels of protection. Once this is achieved,

---

303 Gersdorf, in: BeckOK, *Informations- und Medienrecht*, 20th edition, Art. 8 ECHR marginal note 55.

304 Gersdorf, in: BeckOK, *Informations- und Medienrecht*, 20th edition, Art. 8 ECHR marginal note 58, ECtHR judgement of 23 September 1994 – 19823/92 – Hokkanen/Finland; ECtHR judgement of 25 November 1994 – 18131/91 – Stjerna/Finland.

305 ECtHR judgement of 25 February 1997 – 22009/93 – Z/Finland.

306 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 (Official Journal of the European Communities No L 281/31).

307 Explanations relating to the Charter of Fundamental Rights (Official Journal of the European Union C 303/20 of 14 December 2007).

308 Kühling/Martini (fn. 26) (450); Kühling/Sackmann, "Datenschutzordnung 2018 – nach der Reform ist vor der Reform?!", NVwZ 2018, 681.

309 Recital 7.

the Member States are then prevented from obstructing the free communication of personal data for reasons relating to the protection of the rights and freedoms of natural persons, and in particular the right to privacy. A high level of data protection is therefore less an aim in itself than an instrument for realising the Single Market objective. Nevertheless, the Community aims to implement a high level of protection in the directive, which must not be inferior to that granted in Art. 8 ECHR and the general principles of Community law.[310]

Art. 2(a) of Directive 1995/46/EC defines personal data as any information relating to an identified or identifiable natural person. A person is deemed identifiable if he or she can be directly or indirectly identified. This can be done by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. This means that any reference to income or assets and tax data falls within the scope of personal data and therefore within the scope of application of the directive.

Given that the recitals make reference to the ECHR, it is not surprising that the concept of protection laid down in Directive 1993/46/EC has similarities to that in Art. 8 ECHR. For example, the directive lays down the principle of purpose limitation. The collection and further processing of personal data has not been banned outright, but the data may only be collected and processed for clearly defined, legitimate purposes. In addition to requiring the data subject's consent (Art. 7(a) of Directive 1993/46/EC), the directive allows data processing for, among other purposes, the performance of tasks carried out in the public interest, although this is restricted by making it subject to proportionality. The directive clearly hints at the basic principle of protecting rights by way of organisation and procedures. Examples in this regard include rights of erasure (Art. 7(e) of Directive 1993/46/EC) or the data subject's right to information (Art. 10 ff. of Directive 1993/46/EC) and requirements for the security of processing (Art. 17 of Directive 1993/46/EC).

Art. 13 of Directive 1993/46/EC allows Member States to provide for exemptions from and limitations of certain rights granted in the directive. Pursuant to Art. 13(1)(e) of Directive 1993/46/EC, this also includes an important economic or financial interest of a Member State, including taxation matters. Limitations of this kind must, however, be necessary and are therefore subject to the proportionality principle. Member States are required to provide for variances and exemptions for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression (Art. 11 of Directive 1993/46/EC). This is in turn subject to the principle of proportionality and must prove to be necessary in order to make the right to privacy consistent with the requirements applicable to freedom of expression.

310 Recital 10.

4. Right to respect for private life and protection of personal data (Art. 7, 8 CFREU)

Pursuant to Art. 7 CFREU, everyone has the right to respect for his or her private and family life, home and communications. As evidenced by its wording and history, Art. 7 CFREU recognisably echoes Art. 8(1) ECHR.[311] This entails that the protection granted by Art. 7 CFREU must not be inferior to that provided by Art. 8 ECHR. Art. 8(1) CFREU guarantees everyone the right to protection of the personal data relating to him or her. The categorisation of the two provisions could in fact be argued to suggest that the fundamental right to data protection in Art. 8 CFREU is a special requirement under the guarantee of respect for private life in Art. 7 CFREU.[312] The ECJ, in contrast, seems to assume one consistent fundamental right[313] or investigates the two provisions concurrently.[314] In the recitals to the Charter of Fundamental Rights, reference is made with respect to Art. 8 CFREU to Art. 286 TEEC, Art. 8 ECHR, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Data Protection Directive 95/46/EC.[315] With regard to respect for private life, the protection granted by Art. 7 and 8 CFREU for the processing of personal data extends to any information relating to an identified or identifiable natural person. This can be made more concrete with reference to the legal definition in Art. 2(a) of the Data Protection Directive 1995/46/EC. Even in the context of Art. 7 and 8 CFREU, a person must be considered identifiable, if he or she "can be identified, directly or indirectly".[316]

The right to data protection in Art. 7 and 8 CFREU is not granted completely without limitations.[317] Pursuant to the first sentence of Art. 8(2) CFREU, personal data may be processed if this is done for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Under the principle that more specific law pre-empts more general law, the general limitation provision of Art. 52(1) CFREU should really be pre-empted by Art. 8(2) CFREU.[318] Without dealing with the issue in detail, the ECJ's case law to date has, however, made direct reference to Art. 52(1) CFREU.[319] Accordingly, any limitation on the exercise of rights and freedoms must be laid down by law and respect the essence of Art. 7, 8 CFREU (first sentence of Art. 52(1) CFREU). Subject to

311 Wolff, in: *Frankfurter Kommentar zu EUV, GRC und AEUV*, 2017, Art. 7 CFREU marginal note 3.

312 Johlen, in: Stern/Sachs, *Europäische Grundrechte-Charta, GrCh*, 2016, Art. 8 CFREU marginal note 24.

313 Arguably as stated in ECJ judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 52.

314 See ECJ judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal notes 29, 37.

315 Recitals to the Charter of Fundamental Rights (2007/C 303/02), OJ EU C 303/20 of 14 December 2007.

316 See D.II.3 (p. 76) above.

317 ECJ, judgement of 17 October 2013, C-291/12 (Schwarz), ECLI:EU:C:2013:670 marginal note 33.

318 Bernsdorff, in: *Charta der Grundrechte der Europäischen Union*, 3rd ed. 2014, Art. 8 marginal note 17.

319 ECJ, judgement of 17 October 2013, C-291/12 (Schwarz), ECLI:EU:C:2013:670.; ECJ, judgement of 21 December 2016, C-203/15 (data retention III), ECLI:EU:C:2016:970 marginal note 94.

the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (second sentence of Art. 52(1) CFREU). Since the right to data protection is a subset of the right to respect for privacy, the requirements laid down in the first sentence of Art. 52(3) CFREU should also extend to compliance with the requirements of Art. 8(2) ECHR.[320]

On the basis of everyone's right of access to information on data that has been collected concerning him or her and the right to have it rectified (first sentence of Art. 8(2) CFREU), and the institutional guarantee that an independent authority must be established to monitor compliance with these requirements (Art. 8(3) CFREU), the CFREU gives positive expression to the concept of fundamental rights by way of procedures.

5. General Data Protection Regulation

The last stage, for now, in the development of European data protection law at the standard-setting level is the GDPR,[321] which entered into force on 25 May 2018.[322] New issues arise from its legal nature and the way it interacts with national law (see a). Despite the media attention the GDPR has attracted, its underlying substantive concept follows in the familiar footsteps of the Data Protection Directive 95/46/EC, which it has replaced (see b).[323]

a) Legal nature and interaction with national law

As a regulation, the GDPR has general application, is binding in its entirety and directly applicable in all Member States pursuant to the second paragraph of Art. 288 TFEU. The Data Protection Directive, by contrast, had to be enacted in a two-stage legislative process, since according to the wording of the third paragraph of Art. 288 TFEU, directives are binding on Member States only as to the result to be achieved; they leave the choice of form and methods to the national legislators. On closer analysis, the GDPR is another example of how the differences between the legislative acts of directive and regulation are becoming more and more blurred.[324] The original intention had been to keep the GDPR "lean" and expand on its contents by way of tertiary legislation taking the form of regulations at EU level, but the European Commission was forced to abandon this method in the course of the legislative process.[325] The

320 Johlen, in: Stern/Sachs, *Europäische Grundrechte-Charta, GrCh*, 2016, Art. 8 CFREU marginal note 43.

321 See fn. 47 above.

322 For a selective overview from the almost unmanageable wealth of literature, see Kühling/Martini (fn. 26) ff.; critical view in Veil (fn. 48) ff.

323 Kühling/Sackmann (fn. 309).

324 For a detailed discussion, see Rösch, *Zur Rechtsformenwahl des europäischen Gesetzgebers im Lichte des Verhältnismäßigkeitsgrundsatzes – von der Richtlinie zur Verordnung*, 2013.

325 Albrecht, "Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung", CR 2016, 88 (97).

enabling provisions of the European Commission have been replaced by national regulatory prerogatives, which allow the Member States to implement their own ideas within the limits set by the GDPR. From the perspective of adding democratic legitimacy and respecting national legal culture, these regulatory prerogatives must be welcomed.

It is of course impossible to ignore the fact that the interplay between EU and national law has become significantly more complicated and by no means easier for those having to apply the law. A significant contributing factor is that provisions laid down in EU regulations must not be duplicated elsewhere.[326] The purpose of this prohibition is to make clear the Union character of a provision and thus indirectly protect the ECJ's interpretation monopoly.[327] Even where the GDPR allows the Member States room for clarification and expansion, legislators cannot adopt comprehensive regulations. Instead, they have to limit themselves to a body of regulations that avoids overlap with the GDPR and only fills the space allowed for national discretion. The provisions newly added to the Fiscal Code (Abgabenordnung, AO) for processing personal data by the financial authorities and the information requirements to which they are subject (sections 29b, 29c and 32a of the AO) demonstrate the consequences of this way of regulating, which is not very helpful from a law enforcement perspective. These provisions can only be understood in conjunction with the underlying provisions of the GDPR.[328] However, where national legislators do not make use of the regulatory scope, there are no restrictions for those affected to invoke the directly applicable provisions of the GDPR.

b) Underlying substantive concept of the GDPR

With regard to the underlying substantive legal concept, the GDPR does not mark a completely fresh start, as the data protection concept on which it is based is similar to the one underlying the Data Protection Directive 95/46/EC. Rather than a revolution, it should therefore be termed an evolution of established data protection law.[329]

The consent principle (Art. 6(1)(a), 4(11) GDPR, recital 40)[330] and purpose limitation in principle (Art. 5(1)(b) and (c) GDPR) have been retained. There is no need to discuss other changes that are of practical importance, such as the territorial scope principle (Art. 3 GDPR), tougher sanctions for non-compliance

326 Federal Ministry of Justice, *Handbuch der Rechtsförmlichkeit*, 3rd ed. 2008 marginal note 289.

327 See ECJ judgement of 7 February 1973, C-39/72 (Commission/Italy), Slg. 1973, 101 marginal note 17; ECJ judgement of 10 October 1973, C-34/73 (Fratelli Variola), Slg. 1973, 981 marginal note 9 ff.

328 For an instructive discussion, see Baum, "Datenschutz im Steuerverwaltungsverfahren ab dem 25.5.2018. Teil II: Zulässigkeit der Verarbeitung personenbezogener Daten durch Finanzbehörden", NWB 2017, 3203 ff.; Baum, "Datenschutz im Steuerverwaltungsverfahren ab dem 25.5.2018. Teil III: Informationspflichten der Finanzbehörden und Auskunftsrechte der betroffenen Personen", NWB 2017, 3143 ff.

329 Kühling/Martini (fn. 26).

330 For a critical review of attempts by German commentators to put this into question, see Albrecht (fn. 326) (91).

(Art. 83(6) GDPR), the right to be forgotten (Art. 17 GDPR) and organisational changes, because they are not relevant in the context of this study.

The newly legislated (data protection) transparency requirement (Art. 5(1)(a) GDPR) is of great relevance, on the other hand. Based on this requirement, personal data must be processed not only lawfully and fairly but also in a transparent manner in relation to the data subject. This transparency requirement is explained as follows in recital 39:

> "It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data about them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing."

In expanding on this transparency requirement, the GDPR has created a number of new rights which have to be interpreted and applied in the light of this principle. This includes the specific requirements for the controller's conduct (Art. 12 GDPR), information obligations (Art. 13 f. GDPR) and the data subjects' right of access to the information (Art. 15 GDPR).[331]

331 Frenzel, in: Paal/Pauly/Ernst/Frenzel/Gräber/Hennemann/Körffer/Martini/Nolden, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, 2nd ed. 2018, Art. 5 GDPR marginal note 22.

Pursuant to Art. 4(7) GDPR, a controller is any 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. Pursuant to Art. 13(1)(e) GDPR (information to be provided where personal data are collected from the data subject), the information requirements to be met by the controller also include disclosure of the recipients or categories of recipients of the personal data. In addition, Art. 15 GDPR gives the data subject extensive rights to demand access to the information from the controller. They include the purposes of the processing (Art. 15(1)(a) GDPR), the recipients or categories of recipients to whom the personal data has been or will be disclosed (Art. 15(1)(c) GDPR) and, in principle, the envisaged period for which the personal data will be stored (Art. 15(1)(d) GDPR). In addition to the right to rectification (Art. 16 GDPR), Art. 17(1) gives the data subject the right to erasure of personal data about him or her without undue delay, if the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed (Art. 17(1)(a) GDPR).

c) Balancing against other fundamental rights

There is considerable uncertainty at present about what modifications will be made to the rights to the protection of personal data granted in the GDPR, if they conflict with opposing fundamental rights. The issue is addressed at the beginning of the recitals, which state that the right to the protection of personal data is not an absolute right.[332] Rather, it must be considered in relation to its function in society and be balanced against other fundamental rights in accordance with the principle of proportionality; the rights specified include freedom of expression and freedom of information. These are also protected by the Charter of Fundamental Rights and guaranteed in Art. 11(1) CFREU.

In the normative text of the GDPR, however, this issue is only addressed in chapter IX, which deals with provisions relating to specific processing situations. The relevant provisions are located in Art. 85 GDPR, which governs the processing and freedom of expression and information and requires Member States to lay down legal provisions to reconcile the right to the protection of personal data pursuant to this regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression (Art. 85(1) GDPR).

Art. 85(2) GDPR contains another requirement: For processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression, Member States are required to provide for exemptions or derogations from chapters II-VII and IX if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information. Each Member State has to notify the European Commission of the provisions of its law and, without undue delay, of all subsequent amendments to these provisions which it has adopted pursuant to Art. 85(2) GDPR (Art. 85(3) GDPR).

332 Recital 4.

The controversy about the relationship between paragraphs 1 and 2 of Art. 85 GDPR has not yet been resolved. Conceivable interpretations are that both provisions grant Member States separate powers that are independent of each other, but also that Art. 85(2) GDPR provides final clarification for Art. 85(1) GDPR.[333] This is significant not only for the notification requirements of Art. 85(3) GDPR, but also with regard to the extent of powers to provide for clarifications and exemptions. While Art. 85(1) GDPR does not contain any restriction in this regard, Art. 85(2) GDPR, by itself, allows exemptions from the provisions in chapters II-VII and IX of the GDPR. It is probably correct to assume that these are not two separate regulatory tasks that are independent of each other. Rather, Art. 85(1) GDPR is a general regulatory task and Art. 85(2) GDPR contains rules for exemptions that expand on this task. This means that the task set by Art. 85(1) GDPR to reconcile the competing rights or fundamental rights positions must be completed within the constraints of Art. 85(2) GDPR.[334]

Irrespective of the issue under dispute, Art. 85 GDPR does not, however, give Member States carte blanche to impose any limitations they choose on the level of protection granted by the General Regulation. This is clearly stated in recital 4: the right to the protection of personal data must be balanced against other fundamental rights, in accordance with the principle of proportionality. This calls for careful balancing, which, according to general principles of interpreting secondary law in compliance with primary law, should be based on the values enshrined in the CFREU. This guides attention towards the clarification of Art. 7 and 8 CFREU by way of court rulings, which will be the subject of detailed discussion in the following section (see IV. below).

6. Additive interference with fundamental rights

The issue of "additive interference with fundamental rights"[335] deserves special attention, particularly in a data protection context. The concept has been developed in the case law of the Federal Constitutional Court. The basic idea is that several interferences with fundamental rights that could, in isolation, still be considered permissible may together constitute a violation of fundamental rights, because their negative impact is compounded, thus pushing the effect beyond what is reasonably acceptable. Although the prohibition on additive interference with fundamental rights is not directly codified in the text of the Basic Law of Germany, there are references or at least clear commonalities, such as the requirement to avoid overburdening taxpayers (article 106 (3) sentence 4 no. 2 of the GG), the obligation to guarantee

333 Arguably as stated in Specht, in: Sydow, *Europäische Datenschutzgrundverordnung*, 2nd ed. 2018, Art. 85 marginal note 6.

334 This is supported by the history of its development, because the provision was only "split up" at a relatively late stage (Specht, in: Sydow, *Europäische Datenschutzgrundverordnung*, 2nd ed. 2018, Art. 85 marginal note 6). What is more, if these two regulatory tasks were independent of each other, it would be very hard to explain why the relatively detailed recitals (see recital 153) do not distinguish between the two provisions.

335 For the most recent comments, see Kaltenstein, "Kernfragen des 'additiven' Grundrechtseingriffs unter besonderer Berücksichtigung des Sozialrechts", SGb 2016, 365 ff.

the substance of basic or fundamental rights (article 19 (2) of the GG, first sentence of Art. 52(1) CFREU) and the prohibition on double punishment (article 103 (3) of the GG, Art. 50 CFREU).

The cases to which the Federal Constitutional Court's judgements apply range from social law to tax law. However, the first time the issue was made explicit in the BVerfG's judgements was in 2005 in a data protection law ruling in connection with the accumulation of a number of observation measures.[336] It has since been referred to several times, but has not yet become relevant to any rulings.[337] Perhaps this is the reason why there is still uncertainty about how the concept is classified in terms of legal dogmatics. There are many arguments in support of the presumption that the interference must occur at or at least near the same time and that it has to affect the same individual and the same fundamental right. Where interference is laid down at different levels of the law, this cannot rule out the need to consider its additive effect. If there is additive interference with fundamental rights, an overall proportionality assessment is required. Especially in the area of data protection law, it is plausible that such an assessment is more likely to lead to the assumption of a violation of fundamental rights than a stand-alone assessment. Even seemingly trivial information may provide deep insights into an individual's personality and personal circumstances when considered together with other data, with the result that the extent of the interference of the stand-alone measures is determined not merely by aggregation but by compounding. The fact that the issue has not become relevant to any rulings to date also highlights that the acceptance threshold must be considered relatively high.

In the ECJ's case law, the issue of additive interference with fundamental rights has not been addressed up to now. In view of the lines of reception between the case law of the Federal Constitutional Court and that of the ECJ (see Art. 52 CFREU), there is much to suggest that the ECJ will broach this issue as soon as an opportunity comes up. This applies all the more as the guarantee of the substance of the fundamental rights is also laid down in the Charter of Fundamental Rights.

III. Justified by the transparency principle?

Pursuant to the second paragraph of Art. 1 TEU and the second sentence of the third paragraph of Art. 10 TEU, decisions must be taken as openly as possible and as closely as possible to the citizens. Art. 15 TFEU has a similar remit. This provision stipulates that the European Union's institutions, bodies, offices and agencies must conduct their work as openly as possible; it specifies that the European Parliament must meet in public, requires the European Union's institutions, bodies, offices and agencies to be

336 BVerfGE 112, 304 (320).

337 For details, see decision analyses in Kaltenstein (fn. 336) (366 ff.).

transparent and codifies the right in principle to the publication of documents (Art. 15(3) TFEU). Based on the above principles, the ECJ has derived a transparency principle.[338]

This prompts the question whether interference with privacy and the fundamental right to data protection associated with disclosure requirements can be based on this transparency principle. The answer to this question has to differentiate between different aspects. The transparency principle is aimed at supervising government actions. In order to be effective, such supervision has to be carried out on a sufficient informational basis. This means that there does not seem to be any relation between personal data and the transparency principle with regard to data that is not directly connected to government and administrative actions. Examples in the present context include an individual's income and assets. Any disclosure requirements established in this area cannot be based on the transparency principle without turning the rationale of the institution on its head, as it were.

The various clarifications of the transparency principle in the TEU and TFEU are exclusively aimed at improving oversight over the decisions of the European Union. In contrast, the transparency principle is in no way intended to lead to the disclosure of personal information, as the wording, classification and rationale of its clarifications suggest. The claims established on their basis are exclusively aimed at the European Union's institutions, bodies, offices and agencies, but not at private individuals. This is confirmed by the second subparagraph of Art. 15(3) TFEU, which limits the right of access to documents of the European Union on grounds of private interest. If this limit was removed, an instrument to supervise the exercise of government power would be turned into an instrument of social control that would force private individuals outside the context of justification in a democracy and under the rule of law to justify their personal circumstances and conduct vis-à-vis the public.

The situation for personal data collected to perform sovereign tasks and functions by government authorities and institutions is more complex. Think of tax data, for example, or application documents filed by recipients of state subsidies. If this kind of data is made public, it interferes with the right to informational self-determination of the data subjects, but at the same time serves to supervise the actions of the governmental authorities. The transparency principle can be applied to such cases in principle: in each individual case, it then has to be balanced against competing data protection interests. The ECJ's ruling in the Schecke matter illustrated the policies that have to be observed in this regard; they will be discussed in detail later (see IV.1.c below).

338 ECJ judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 75 (see IV.1.c below for more details).

IV. Lines of development

The ECJ was initially very reluctant to deal with issues of data protection. One example is the first ruling on data retention handed down in 2009, in which the court had limited itself to a test in terms of competency powers without addressing the fundamental rights dimension.[339] For a number of years, the earlier reluctance has given way to an attitude that is no longer characterised by judicial self-restraint but judicial activism.[340] Today, the ECJ's data protection standards are no longer lower than those set by the Federal Constitutional Court, and in some case they even exceed them. The path to this new policy has been marked by key landmark rulings; they will be discussed briefly below and their relevance for weighing disclosure requirements against data protection will be demonstrated.

1. Landmark rulings

a) ECJ/Austrian Court of Auditors (2003)

The ruling on the case of the Austrian Court of Auditors (Rechnungshof) dates back to 2003. The ECJ was asked to decide by way of a preliminary ruling process whether the fact that government institutions have to report income data about their employees to the Austrian court of Auditors for the purpose of publication was compatible with Community law on data protection. The ECJ did not give its own answer to the question, but gave the national courts balancing directives to enable them to test the proportionality of the interference with privacy as protected by Art. 8 ECHR associated with disclosure and whether that is compatible with the Data Protection Directive 95/46/EC.

The presumption of interference with privacy and the collection of personal data is not precluded by the fact that the disclosure requirement relates to professional activities.[341] A touchstone as to whether national law is compatible with the directive is whether there is advance warning of any interference. In the terminology used by the Federal Constitutional Court, advance warning is equivalent to the requirement for clear legal arrangements that apply to a specific area for any interference with informational self-determination.[342] Furthermore, under the principle of proportionality, a careful check is required to establish whether there is a less intrusive alternative to disclosing the data to the public.[343] Options mentioned in this regard are to limit the disclosure of data to the Court of Auditors and to redact data

339 ECJ, judgement of 10 February 2009, C-301/06 (Ireland v Commission), Slg 2009, I-593 marginal note 57.

340 Very instructive discussion in Skouris (fn. 22) ff.; see Hornung, "Anmerkung zum Urteil des EuGH vom 9.11.2010 (C-92/09; C-93/09, MMR 2011, 122) – Datenschutz und Veröffentlichung von Empfängern von EU-Agrarsubventionen im Internet", MMR 2011, 127 ff.

341 ECJ, judgement of 20 May 2003, C-465/00, C-138/01 and C-139/01 (Österreichischer Rundfunk), Slg 2003, I-4989 marginal note 73.

342 ECJ, judgement of 20 May 2003, C-465/00, C-138/01 and C-139/01 (Österreichischer Rundfunk), Slg 2003, I-4989 marginal note 78.

343 ECJ, judgement of 20 May 2003, C-465/00, C-138/01 and C-139/01 (Österreichischer Rundfunk), Slg 2003, I-4989 marginal note 88.

to be disclosed to the public by removing information that permits conclusions about the personal and family situation of the data subject.

b) ECJ/Satamedia (2008)

Upon submission by a Finnish appeal court, the ECJ was asked to rule in the Satamedia case in 2008 whether the publication of tax data was compatible with the Data Protection Directive 95/46/EC. Data had been made public by a private company that published public data available from the tax authorities in Finland. The information, which was set out in the form of an alphabetical list of residents and organised according to municipality, included the amount of income and taxation on the residents' assets. At the same time the data had also been made accessible for dissemination by a text messaging service. To justify its actions, the provider had invoked the exemption and derogation for journalistic purposes provided for in Art. 9 of Directive 95/46/EC.

First, the ECJ determined that the publication related to personal data, i.e. data on an identified or identifiable person.[344] When weighing up the competing fundamental rights positions, the ECJ stated that, on the one hand, the term of journalism required a broad interpretation owing to its connection with freedom of expression while, on the other hand, the protection of privacy necessitated that any exemptions and limitations in relation to data protection were limited to what is strictly necessary.[345] The national court then had the responsibility of conducting its own review of this. Another unusual aspect of the ruling is that the arguments pertain exclusively to the level of secondary law without establishing a link to the conflicting fundamental rights underlying the directive. As a result, the ruling as a whole shows unusual judicial restraint.

c) ECJ/Schecke (2010)

In the Schecke ruling of 2010, the ECJ made it abundantly clear how seriously even secondary legislators had to take data protection. The court had been asked to rule on whether it was permissible to publish online the names of recipients of agricultural aid and the amounts they had received.[346] Online publication was governed by Regulation (EC) No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD). The ECJ found that the publication requirement in relation to natural persons was a violation of Art. 7 and 8 CFREU.

The publication requirement is aimed at enhancing transparency regarding the use of Community funds and improving the sound financial management of these funds. As such, the legislator can invoke the

344 ECJ, judgement of 16 December 2008, C-73/07 (Satamedia), Slg 2008, I-9831 marginal note 35.

345 ECJ, judgement of 16 December 2008, C-73/07 (Satamedia), Slg 2008, I-9831 marginal note 56.

346 ECJ, judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR).

transparency principle enshrined in principle by the ECJ in Art. 1 and 10 TEU and in Art. 15 TFEU. The transparency principle is aimed at improving citizens' involvement in the decision process and ensuring that the administration shows greater legitimacy, efficiency and accountability to citizens in a democratic system.[347] The suitability of the intervention is not being denied. Publication strengthens oversight of the use of the amounts involved and contributes to ensuring that public funds are used in the best possible way.[348]

The validity of the regulation is called into question by the fact that its provisions are not necessary. The ECJ bases this view on the principle developed in the Satamedia ruling, according to which exemptions and limitations in relation to the protection of personal data must be limited to what is strictly necessary.[349] In a departure from the understanding of the Federal Constitutional Court, the need is then interpreted procedurally. The failure to meet the necessity requirement was thus not due to the fact that the publication of names was not necessary, but that the institutions of the European Union should have examined whether limited publication by name would have been sufficient to meet the legislative objectives.[350]

d) ECJ/data retention II/III (2014/2016)

Two ECJ rulings on data retention, handed down in 2014 and 2016, are another milestone in the court's case law on data protection.[351] The subject of the first ruling was Directive 2006/24/EC, which intended to require providers and operators of publicly available electronic communications services to retain communications data itemised in the directive in order to make this data available to the competent national authorities, if necessary. This directive also failed because of disproportionate interference with the data protection guarantees of Art. 7 and 8 CFREU. At the same time, the court made an examination and found a violation of the freedom of expression protected by Art. 11 CFREU.

This assessment is significant for at least two reasons: firstly, in this specific case, the ECJ considers data protection more important than the objectives of combating organised crime and terrorism pursued by EU legislators, even though the fight against serious crime is of the utmost importance for guaranteeing public safety and the ECJ concedes at the same time that the effectiveness of the fight against crime can depend to a large extent on the use of modern investigation techniques.[352] Despite these reservations,

---

347 ECJ, judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 68.

348 ECJ, judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 75.

349 ECJ, judgement of 16 December 2008, C-73/07 (Satamedia), Slg 2008, I-9831 marginal note 56.

350 ECJ, judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 83.

351 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238; ECJ, judgement of 21 December 2016, C-203/15 (data retention III), ECLI:EU:C:2016:970.

352 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 51.

it argued that these objectives in the general interest, however fundamental they may be, could not by themselves justify the need for data retention for the purpose of fighting crime.

Secondly, the ECJ's ruling is a departure from the procedural understanding of the principle of proportionality.[353] Unlike the Schecke ruling, the failure of proportionality is no longer due only to the fact that the European Union's institutions have neglected to examine possible less onerous alternatives to establish whether they are equally suitable for meeting the pursued objectives. Instead, the ECJ calls for minimum requirements intended to guarantee effective protection of personal data against the risks of misuse, any unauthorised access and any unauthorised use.[354] The ECJ assessed that the interference would be exacerbated by the extent of the data collected as well as the fact that data could be used without the subscriber or registered user being informed and could thus generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance.[355]

Another circumstance exacerbating the interference is that the data is collected without a valid cause, because data is included even about persons for whom there is no evidence to suggest that their conduct might have a link, even an indirect or remote one, with serious crime.[356] The same applies to the breadth of the interference, because the directive did not specify data retention in any detail pertaining to a particular time period, geographical zone or circle of particular persons.[357] Other circumstances exacerbating the interference included the failure of the directive to make access to the data dependent on a prior review carried out by a court or by an independent administrative body in order to limit its use to what is strictly necessary to pursue the objective.[358] Furthermore, Art. 8 CFREU required guarantees that the data retained would be effectively protected against the risk of abuse and against any unlawful access and use of that data. It was necessary to have rules in place which would serve to govern the protection and security of the data in question in a clear and strict manner, and EU legislators had failed to ensure that.[359] And lastly, Art. 8(3) CFREU specified that the data protection and data security requirements had to be monitored by an independent authority.[360]

---

353 Instructive comments on how to categorise the ruling in Pache, in: Pechstein/Nowak/Häde/Boysen, *Frankfurter Kommentar zu EUV, GRC und AEUV*, 2017, Art. 52 CFREU marginal note 29.

354 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 54.

355 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 37.

356 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 59.

357 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 59.

358 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 52.

359 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 66.

360 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 68.

The strong emphasis on data protection received another boost in 2016 in what was probably the last ruling for now on the permissibility of data retention. In the preliminary ruling procedure, the ECJ had been asked to rule on the compatibility of data retention based on national law with the Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive 2002/58/EC). Art. 15 of Directive 2002/58/EC allows Member States, among other things, to grant exemptions from the prohibition on traffic data retention, if this is necessary for reasons of public security and the pursuit of criminal offences in a democratic society. In this way, the directive makes data retention subject to proportionality, a requirement that already applied from a fundamental rights perspective.

Among the fundamental rights affected, the ECJ singles out not only the protection of privacy (Art. 7 and 8 CFREU), but also the guarantee of freedom of expression (Art. 11 CFREU). With reference to preliminary rulings, the court then confirms that exemptions from limitations on the protection of personal data must be limited to what is strictly necessary.[361] With reference to the preliminary ruling, this is negated using the arguments that had prompted the ECJ to declare the Data Retention Directive invalid.

A consequence of this ruling is that, irrespective of the considerable threats and risks associated in particular with organised and international crime, extensive traffic data retention cannot be implemented, even at the national level. Through this ruling, the ECJ has set much tighter limits for the scope of security policy and police law of the Member States than the Federal Constitutional Court, which considers data retention permissible in principle, provided the applicable guarantees under the rule of law are met.[362]

e) Side note: decision of the Conseil constitutionnel of 8 December 2016

In its decision handed down on 8 December 2016, the Conseil constitutionnel (Constitutional Council of France) declared public country-by-country reporting laid down in French law unconstitutional, although in the banking sector this requirement was in part based on EU rules. The grounds for the decision do not deal with the data protection issue in any more detail, meaning that the decision does not directly affect the subject under investigation in this study. However, since the issues are closely related, a brief summary of the decision will be presented here.

In the grounds for the decision, which are kept very brief in line with French legal tradition, the Constitutional Council concedes that, given its aim of fighting tax evasion and tax avoidance, the requirement to publish CbCR had a legitimate objective.[363] However, the provisions constituted disproportionate interference with the freedom to carry on a business. For example, public CbCR could give business

361 Schenke, in: Stern/Becker, *Grundrechte-Kommentar*, 3rd ed. 2018, article 10 of the GG.

362 BVerfG, judgement of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (data retention), BVerfGE 125, 260.

363 Conseil constitutionnel of 8 Dec. 2016, 2016-741 DC marginal note 102.

partners and competitors access to key elements of the production and distribution structure.[364] The Council does not provide any more detailed arguments.

From an EU law perspective, the decision allows only very limited conclusions about how it assesses CbCR.[365] It could initially be argued that Art. 16 CFREU also protects the freedom to carry on a business, which is negatively affected if a company has to give its competitors indirect access to its business strategy through public CbCR.[366] It must be conceded, however, that the ECJ grants the European Union institutions wide scope for weighing up alternatives, especially in cases of complex economic matters.[367] Moreover, in more recent, in some cases spectacular rulings, the ECJ did not make any reference at all to the test of freedom to carry on a business.[368] Compared with the strong emphasis on data protection, this aspect can therefore be assumed to play a very minor role. To use it to justify a veto position against public CbCR would require a paradigm shift in the ECJ's case law, similar to the change that occurred in data protection law. There are, however, no signs at present that the development in the area of Art. 16 CFREU will follow along the same lines.

2. Central issues in weighing data protection interests

How fundamental rights should be balanced against opposing public or private interests and rights in the context of the proportionality test required by Art. 52(1) and Art. 8(2) CFREU depends critically on how interference with fundamental rights is weighted. The more seriously the fundamental right is affected, the greater must be the weight of the competing interests.

What is probably the most convincing theory available about how the ECJ's decision practice can be reconstructed touches on the theory of movable systems associated with the Austrian civil law scientist Walter Wilburg.[369] To rationalise a complex balancing decision, the relevant aspects are first identified and then weighted according to their specific significance. In this way, an aspect that has a high ranking

364 Conseil constitutionnel of 8 Dec. 2016, 2016-741 DC marginal note 103.

365 See detailed information in Wöhrer (fn. 19), 25 ff.

366 See detailed and critical comments in Dutt/Spengel/Vay, *Der EU-Vorschlag zum Country-by-Country-Reporting im Internet*, 2017, p. 20 ff.

367 See e.g. ECJ, judgement of 5 October 1994, C-280-93 (Bananas), Slg. 1994, I-4973 marginal note 89.

368 Kühling in: Pechstein/Nowak/Häde/Boysen, *Frankfurter Kommentar zu EUV, GRC und AEUV*, 2017, Art. 16 CFREU marginal note 17.

369 Wilburg, *Entwicklung eines beweglichen Systems im bürgerlichen Recht*, 1950, p. 22; Michael, *Der allgemeine Gleichheitssatz als Methodennorm komparativer Systeme*, 1997, p. 50 ff.; Petersen, *Unternehmenssteuerrecht und bewegliches System*, 1999.

in abstract terms may possibly be outweighed by another opposing aspect with a lower ranking, if the latter proves particularly relevant to solving a factual problem.[370]

Relevant aspects qualifying for the assessment under data protection law include the general weighting of data protection (see a) and the concept of protection (see b). These and other balancing criteria (see c to g) will be discussed below.

a) General weighting of data protection

The boost that data protection has received in the ECJ's recent case law[371] can be explained clearly on the basis of its judgements on the general balancing directive. As recently as the Lindqvist ruling handed down in 2003, the ECJ only required that a fair balance must be maintained between data protection and competing interests.[372] National case law has to date reflected a similar assessment.[373] In contrast, the ECJ's line of jurisprudence, which started in the same year, adopts a much stricter way of judging. Since the Satamedia ruling, the court has demanded that exemptions from the protection of personal data and limitations of the fundamental right must be applied only in so far as is "strictly necessary".[374] By choosing this wording, it postulates a rule-exemption ratio that makes restrictions of data protections an exception for which an explanation must be provided. The potentially equal balance between data protection and other competing interests has thus been superseded by the primacy of data protection.

b) From a procedural to a substantive protection concept

The tightening of the control standard is accompanied by the realignment of the protection concept, which was originally based on a procedural approach. This is characterised by the fact that the legislators' scope for assessment is reined in by imposing a procedural burden of justification rather than by specifying binding content. The Schecke ruling makes this point particularly clearly. The grounds for the decision suggest that the directive on the disclosure of recipients and amounts of agricultural subsidies was ruled invalid not because the result of balancing the different interests was incompatible with fundamental rights, but because the requirements to examine the different fundamental rights interests

370 Schenke, in: Stern/Becker, *Grundrechte-Kommentar*, 3rd ed. 2018, article 10 of the GG.

371 Weismantel, *Das 'Recht auf Vergessenwerden' im Internet nach dem 'Google-Urteil' des EuGH*, 2017, p. 48 f.

372 ECJ, judgement of 06 November 2003, C-101/01 (Bodil Lindqvist), Slg 2003, I-12971 marginal note 85.

373 BGH, judgement of 8 February 1994, VI ZR 286/93, NJW 1994, 1281; BVerfG, decision of 3 May 1994, 1 BvR 737/94, NJW 1994, 1784 (1785).

374 ECJ, judgement of 16 December 2008, C-73/07 (Satamedia), Slg 2008, I-9831 marginal note 56; ECJ, judgement of 9 November 2010, C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 77; ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 52; ECJ, judgement of 6 October 2015, C-362/14 (Schrems), ECLI:EU:C:2015:650 marginal note 92.

and to justify any restrictions had not been met.[375] This suggests that the specific weighting would have been approved by the ECJ if it had appropriately taken account of the need to impose such far-reaching disclosure requirements and the inadequacy of more lenient measures.

Starting with the second ruling on data retention, the procedural protection concept was replaced or complemented by a substantive approach. Unlike the Schecke ruling, the ECJ bases its decision not only on the EU legislators' failure to meet their examination obligation adequately, but also makes it very clear that the retention of content data could generally not be justified, no matter how high the priority of the objectives pursued. The trust that, in an informed political process that takes data protection sufficiently into account, only those solutions will prevail that do not limit data protection any further than is strictly necessary has been replaced by mandatory data protection requirements. The result is a significant boost for data protection and in turn a decline in political flexibility.

c) Inclusion of the professional domain

Company-related disclosure requirements must be capable of being tested against the right to respect for private life protected in Art. 7 and 8 CFREU. The ECJ's settled case law rejects the exclusion of profession-related data from the rights protected by Art. 7 and 8 CFREU.[376] The fact that company-related disclosure requirements affect the professional domain cannot call into question the protection to be granted pursuant to Art. 7 and 8 CFREU. There is no reason to doubt this core statement. Attempts to put a clear break between personal data from the more immediate private domain and personal data from the professional domain would cause problems of demarcation that would be very difficult to solve. They would also fail to account for the fact that an individual's professional and economic domain is a key element in the development of his or her personality. This is especially true for family businesses, where corporate governance is often an expression of family culture and family identity passed down through generations so that the professional and private domains are two sides of the same coin. This is why the ECJ's judgements, which have ruled that tax data in particular is protected by Art. 7 CFREU, deserve unqualified approval.[377] An assessment of the disclosure requirements in the transparency register would not come to any different conclusion. The fact that it entails the disclosure of economic activities does not alter the need to protect the individuals concerned. A citizen's business activities also fall under the protection of the fundamental rights governed by Art. 7 and 8 CFREU.

---

375 ECJ, judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 83: "The institutions ought thus to have examined, in the course of striking a proper balance between the various interests involved, whether publication by name limited in the manner indicated in paragraph 81 above would have been sufficient to achieve the objectives of the European Union legislation at issue in the main proceedings."

376 ECJ, judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 59; ECJ, judgement of 20 May 2003, C-465/00, C-138/01 and C-139/01 (Österreichischer Rundfunk), Slg 2003, I-4989 marginal note 73 f.

377 ECJ, judgement of 1 October 2015, C-201/14 (Bara), ECLI:EU:C:2015:638 marginal note 29; ECJ, judgement of 16 December 2008, C-73/07 (Satamedia), Slg 2008, I-9831 marginal note 35.

d) Sensitivity continues after disclosure

As shown above, commercial, company and capital market laws have laid down disclosure requirements for some time.[378] By contrast, disclosure requirements are still unknown in German tax law. It is too early to tell whether the European Commission's proposal to develop the current country-by-country reporting into public country-by-country reporting will prevail in the subsequent legislative process.[379] However, the mandatory requirement of publicly disclosing personal data conceivably represents the most serious interference with the protected fundamental right to privacy. Even where case law has not called into question in principle that disclosure requirements are compatible with fundamental rights, it has not set aside the sensitivity of personal data. This principle has been recognised in the judgements handed down by the ECJ, the ECtHR as well as the Federal Constitutional Court. For the ECJ and the ECtHR, reference can be made to the Satamedia ruling[380] outlined above and the ECtHR's follow-up ruling[381].

As mentioned earlier, a similar ruling by the Federal Constitutional Court was handed down as early as in 1994. In this case, the BVerfG had been asked to rule on a business administration professor's right to use the annual financial statements of a construction company published in the Federal Gazette for training purposes without anonymising the document. As the BGH before it, the BVerfG rejected this right[382]. Protection of the general right of personality or of commercial freedom – the equivalent right for legal persons – is not suspended by the fact that annual financial statements are publicly accessible pursuant to sections 325 ff. of the HGB.[383]

If personal data enjoys protection as a fundamental right after it has been disclosed, it follows that legislators continue to have a duty to protect this data against uses other than those covered by the original purpose of collecting it.

e) Extent of interference

A factor that exacerbates the severity of interference in privacy protected as a fundamental right is the extent of the interference. This assessment is likewise supported by judgements of the Federal Constitutional Court and similar judgements of the ECJ and the ECtHR. In the two latest rulings on data retention, the ECJ criticises the fact that the directive and the national regulations do not provide for any

378 For details, see assessment in part C.I. above (p. 19 ff.).

379 See C.III.3 (p. 64) above.

380 ECJ, judgement of 16 December 2008, C-73/07 (Satamedia), Slg 2008, I-9831.

381 ECtHR, judgement of 27 June 2017, 931/13, NLMR 2017, 264 marginal note 138.

382 BGH, judgement of 8 February 1994, VI ZR 286/93, NJW 1994, 1281.

383 BVerfG, decision of 3 May 1994, 1 BvR 737/94, NJW 1994, 1784.

differentiation, limitation or exemption, depending on the objective pursued.[384] Instead, data retention indiscriminately affects all individuals who use electronic communications services, even though these individuals are not even indirectly in a situation that could give rise to criminal prosecution. The ECJ's criticism is thus levelled at the number of individuals and issues affected by the interference and the fact that it is conducted without a valid cause. In its judgement handed down as early as 2010, the BVerfG had made a very similar ruling, arguing that the interference had been particularly serious because of its extent.[385] The decision by the ECtHR on tax transparency in Finland, which was published in 2017, follows the same line of argument. In this case, the court also bases its decision mainly on the fact that the information published by the complainant company was not limited to a specific group of persons with a special relevance to the claimed journalistic interest.[386]

f) Feeling of constant surveillance

The ECJ deemed that, where informational interference by the state generates the feeling of being under constant surveillance, this exacerbates the seriousness of the interference. The ECJ developed this issue in the second data retention ruling and referred to it again in the third ruling.[387] In this context, the second ruling refers explicitly to the opinion of the Advocate General, who pointed out the interference with exercising the right to freedom of opinion and expression by the citizens of the European Union.[388] The Advocate General's opinion refers in turn to judgements of the Federal Constitutional Court, according to which a vague feeling of being watched may impair the uninhibited exercise of fundamental rights in many areas.[389]

g) Procedural safeguards against misuse of personal data

A central pattern of consensus of how interference with privacy as a fundamental right can be made less intrusive and thus justifiable in terms of constitutional law requirements is provided by organisational and procedural safeguards, which in the BVerfG's judgements are derived from the proportionality

384 ECJ, judgement of 21 December 2016, C-203/15 (retention data III), ECLI:EU:C:2016:970 marginal note 105; ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 57 f.

385 BVerfGE 125, 260 marginal note 210, 338 (Schluckebier dissenting opinion); instructive comments on the analysis of the criterion in Held, *Intelligente Videoüberwachung*, 2014, p. 131 ff.; from the BVerfG's case law, see BVerfGE 115, 320 (354, 356); 113, 29 (53); 113, 348 (383).

386 ECtHR, judgement of 27 June 2017, 931/13, NLMR 2017, 264 marginal note 180.

387 ECJ, judgement of 21 December 2016, C-203/15 (retention data III), ECLI:EU:C:2016:970 marginal note 100; ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 37.

388 AG Villalón ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 52.

389 BVerfG, judgement of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (data retention), BVerfGE 125, 260 marginal note 212.

principle.[390] The ECJ's recent case law also follows this line of thought, arguing that informational interference requires the codification of requirements at EU level not only under substantive law but also under procedural law.[391]

What safeguards are required and expedient is dependent on the type and intensity of the intervention in each individual case. Possible safeguards could include rights to be heard, information requirements, control prerogatives (for example on the basis of the exclusive authority of a judge or head of an authority), erasure requirements and documentation requirements. In addition to the specific content, the legislative level is of decisive importance: to ensure equal protection levels throughout Europe, the safeguards of fundamental rights must be set out in EU secondary law and must not be left to the Member States' own initiatives.

V. Analysis and individual assessment

The ECJ's case law on data protection has undergone turbulent changes in recent years. Its initial approach, largely characterised by judicial restraint, has been replaced by judicial activism, which curtails to a significant extent the European Union's scope to interfere excessively with the right to privacy. This shows that earlier stereotypes, in particular the description of the ECJ as an "engine of integration"[392], lacked complexity. In the interest of integration, for a long time the ECJ may have tended to marginalise the scope granted to Member States while stretching that of European institutions. But the court's recent judgements, at least in the area of data protection, have rendered this view obsolete. The ECJ is increasingly seeing its role as a court of fundamental rights which robustly argues for the independent nature of fundamental rights even vis-à-vis EU legislators and in cases where this frustrates hard-won attempts at political integration.

The ECJ's three rulings on data retention are an impressive example demonstrating this paradigm shift. While the first ruling was fully in line with the old pattern of interpretation as a court of integration[393] and ignored data protection aspects, the two subsequent rulings mark a 180-degree turn.[394] From a fundamental and data protection rights perspective, the court has been converted "from Saul to Paul"

390 Most recently e.g. BVerfG, judgement of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09 (BKAG), BVerfGE 141, 220 marginal note. 171.

391 ECJ, judgement of 21 December 2016, C-203/15 (retention data III), ECLI:EU:C:2016:970 marginal note 118; ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 61.

392 Stein, in: *Die Hochschullehrer der Juristischen Fakultät der Universität Heidelberg, Richterliche Rechtsfortbildung*, 1986, p. 619.

393 ECJ, judgement of 10 February 2009, C-301/06 (Ireland v Commission), Slg 2009, I-593.

394 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238; ECJ, judgement of 21 December 2016, C-203/15 (data retention III), ECLI:EU:C:2016:970.

and now defends data protection against limitations even when they are justified on the basis of protection against high-level rights and legal interests – such as the fight against terrorism and other types of extremely serious crime.

If we think recent data protection case law, as analysed above, through to its conclusion, both the establishment of the transparency register (see 1.) and the possible introduction of country-by-country reporting (see 2.) will be subject to considerable objections under data protection law.

1. Transparency register

By establishing the transparency register, EU legislators want to make it more difficult for potential future criminals to hide behind the structure of a company; the register is thus intended to help in the fight against money laundering, terrorism financing and organised crime.[395] In order to meet these objectives, the Fourth and Fifth Money Laundering Directives accept considerable interference with privacy as a fundamental right and the fundamental right to data protection (Art. 7 and 8 CFREU). The intention for MLD 2018 is to require unrestricted public disclosure of the data recorded in the transparency register on beneficial owners for all commercial enterprises.

This interference will have particularly severe consequences because, in combination with the requirement to publish annual financial statements laid down in commercial law, it exacerbates the effect on fundamental rights. When analysed in combination, this data enables reliable conclusions to be made about the income and assets of the beneficial owners. This will expose beneficial owners to an increased risk of becoming the victims of crime, such as extortion or kidnapping. An obligation to give third parties access to information on income and assets may also impact on the spontaneous nature of social interaction in a multitude of ways. Moreover, disclosure of the individuals' financial situation exposes those concerned to the risk of inappropriate public debate of their financial circumstances.

Wealthy individuals therefore have a legitimate interest in deciding freely to whom information on their income and assets is disclosed. The establishment of the transparency register will impair this freedom to a significant extent. The European Commission's qualifying remark that only commercial enterprises would be affected is irrelevant in this context because, as has been shown, even commercial and company-related data is subject to the data protection regime. This applies all the more to family businesses, where the investment in the company is not only the result of an economic interest, but also reflects the holder's close association with the family.

The limit on limitations of the second sentence of Art. 52(1) CFREU serves to protect the holders of the fundamental rights. Subject to the principle of proportionality, limitations may be imposed only if they

395 Recital 14 to Directive 2015/849.

are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. As demonstrated above, when assessing interference with fundamental data protection rights, the ECJ applies particularly stringent tests, which require that the interference is limited to what is "strictly necessary".[396]

With regard to the transparency register, the objectives pursued by legislators – the fight against money laundering and terrorism financing – have been recognised in primary law (Art. 3(2) TEU, Art. 67(1) TFEU) and their legitimacy in principle is not in dispute.

And there are no doubts in principle, at least for now, as to the suitability of the measures. For a measure to be suitable, it is not necessary to choose the most effective instrument, but it can be sufficient that the interference with the fundamental right is (merely) beneficial to the intended objective.[397] Due to lack of experience to date, the scope for assessment given to legislators must also be taken into account in this context, meaning that criticism of potential circumventions or misuses cannot be called into question in principle.

In contrast, the need to establish the transparency register has to be viewed in a much more critical light – at least in connection with the provisions for public access for everyone set out in MLD 2018. The ECJ's second and third data retention rulings provide some guidance in this regard, as almost all the criteria the ECJ applied as touchstones of the permissibility of data retention[398] can also be applied to the transparency register. The only exception is probably the volume of data collected, since data retention affects almost every citizen, while the transparency register only applies to a small section of the population. This is exacerbated, on the other hand, by the fact that data on income and assets of the data subjects is significantly more relevant as personal data.

Furthermore, it continues to seem unsound that EU legislators introduced tighter regulations in MLD 2018 without first waiting for feedback on the implementation of MLD 2015. For comparison, it may be helpful to recall the ECJ's Schecke ruling: If the ECJ mandates that the Council and the Commission weigh up the affected interests of the European Union and the fundamental rights of the data subjects in a balanced manner before writing disclosure requirements into law,[399] this means that the existing instruments must be evaluated before new measures are resolved that exacerbate the interference. Not even the Financial Action Task Force (FATF) calls for a public transparency register in its International

396 ECJ, judgement of 16 December 2008, C-73/07 (Satamedia), Slg 2008, I-9831 marginal note 56.

397 Pache in: Pechstein/Nowak/Häde/Boysen, *Frankfurter Kommentar zu EUV, GRC und AEUV*, 2017, Art. 52 CFREU marginal note 26.

398 See D.IV.1.d) (p. 88) above.

399 ECJ, judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 79.

Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. According to the FATF, the decisive criterion is that the company must hold the information on the respective beneficial owners and is able make it available to the competent authorities at short notice.[400] If European legislators go beyond this standard by introducing a publicly accessible transparency register, this should be preceded by a careful needs analysis to demonstrate that there is no alternative with a similar effect to this increased interference with the right to informational self-determination, and provide the reason for such a conclusion.

A key objection to the substance of the establishment of a transparency register – which is intended to be public in future, and even now is virtually public because it gives NGOs and journalists access – is the fact that data is collected and communicated even about persons for whom there is no indication that they are suspected of money laundering or other crimes. An aggravating factor is that EU legislators can be accused of contradicting themselves in this regard. If the directive otherwise follows a risk-based approach,[401] it is difficult to understand why those who are obligated to be included in the register are indiscriminately exposed to general suspicion as a result of the communication of their data. This is why a much more differentiated arrangement is required that distinguishes at least on the basis of sector or, to be more convincing, bases inclusion on the data subjects' prior conduct. The fact that the transparency register pursues high-level objectives of the European Union cannot be used as an argument against this either. The same applied to the Data Retention Directive, which was nevertheless declared invalid because it violated Art. 7 and 8 CFREU.

Irrespective of the problem that there is no valid cause for the interference, the question arises as to the legitimacy of opening the transparency register to non-authorities. Such access still seems acceptable for NGOs and journalists – assuming sufficient data protection safeguards are in place (more on this below). As representatives of civil society or the Fourth Estate, they perform important functions in society, which are recognised in primary law, e.g. in Art. 15(1) TFEU (participation of civil society) and in Art. 11(2) CFREU (media and press freedom). Their relevance to society must not be underestimated, as the recent examples of the Luxembourg leaks and the Panama and Paradise papers have shown, where investigative journalism drew attention to serious social injustices that the authorities had failed to notice, in some cases for decades.

Much more problematic is the general and unconditional access to the transparency register now being planned in MLD 2018. While it can be assumed that NGOs and journalists will meet due diligence requirements under civil society and press laws, these safeguards will be removed if the transparency register becomes freely accessible. This cannot be justified even by basing it on a general transparency

400 FATF (2012-2018), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html (p. 85).

401 Recital 22 to Directive 2015/849.

principle. We should be mindful of the fact that the basic idea of transparency is to monitor government power.[402] Similar to the principle of the division of powers, this is a formal safeguard that provides a relative guarantee that government powers are not abused, but exercised with democratic accountability to the electorate. This is the only meaning of the transparency principle that has been accepted into the European Treaties. Thus Art. 1 and 10 TEU and Art. 15 TFEU specify that the decisions of the Union should be made openly and close to its citizens. Transparency can in no way be interpreted as a comprehensive requirement for EU citizens themselves to be open among each other. A disclosure requirement as an instrument of mutual social supervision does not comply with the letter or spirit of EU law. To read it as such would fatally contradict the guarantee of privacy and data protection (Art. 7, 8 CFREU); in addition, it would literally have to turn the basic idea of transparency into its opposite. An instrument to control state power would be turned into an obligation on citizens to justify the exercise of their rights to freedom vis-à-vis others, thus fundamentally calling into question the primacy of freedom as a fundamental right. Making a register with such sensitive personal data accessible without imposing any conditions is a failure to recognise that social control means the exercise of power, which is only acceptable under the rule of law if it is limited by fundamental rights protections – or at least made subject to equivalent safeguards. These criteria can no longer be met if unconditional access to the transparency register is given to everyone.

In addition to this objection in principle, MLD 2018 has considerable shortcomings in the area of procedural protection of fundamental rights. Again, the issue can be linked seamlessly to the ECJ's case law on data retention. With regard to data protection safeguards, the ECJ clearly rejected the idea of a theoretically feasible division of powers between the European Union and Member States. Where the directive allows interference with the rights guaranteed in Art. 7 and 8 CFREU, it must itself lay down "clear and precise rules" in order to guarantee that the interference "is actually limited to what is strictly necessary".[403] EU legislators cannot take refuge in the argument or blindly assume that the Member States will ensure adequate protection levels when implementing the directive. Similar to the requirement for clear legal arrangements that apply to a specific area in the BVerfG's case law, EU legislators themselves have an obligation to ensure the necessary protection of fundamental rights.

Set against these obligations, the directive is expected to fall considerably short of the requirements of Art. 7 and 8 CFREU. Art. 30(5) MLD 2015 merely specified that access to information on beneficial ownership could be made subject to prior registration. But even this highly rudimentary provision was not retained in Art. 30 MLD 2018. It reads as follows:

402 For more on the conceptual roots of the transparency principle, see B.II above (p. 12).

403 ECJ, judgement of 8 April 2014, C-293/12, C-594/12 (Digital Rights Ireland Ltd), ECLI:EU:C:2014:238 marginal note 65.

> "Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:
> (a) competent authorities and FIUs, without any restriction;
> (b) obliged entities, within the framework of customer due diligence in accordance with Chapter II;
> (c) any person or organisation that can demonstrate a legitimate interest."

At the level of the EU legislative act, there are no procedural safeguards against this unrestricted requirement to disclose data to everyone. Art. 30(5a) MLD 2018 merely allows Member States to choose to make access to the information held in their national registers conditional upon online registration.

Apart from that, the protection of data subjects is also addressed in Art. 30(9) MLD 2018. It allows Member States on a case-by-case basis to provide for an exemption from access to all or part of the information where this, in exceptional circumstances, would expose the beneficial owner to disproportionate risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, or where the beneficial owner is a minor or otherwise legally incapable.

There is no plausible reason why both safeguards are optional rather than obligatory, because there is a risk that some Member States will opt not to have any such safeguards at all. The lack of protection will also affect citizens of other Member States, if they were to qualify as beneficial owners of a company whose registered office is in the country concerned and who would therefore have to be included in that country's transparency register according to its rules. Without registering access, there is no practical way to ensure that, once collected, the data is only used for the originally intended purpose. Furthermore, it is completely inexplicable that the data can be communicated even in cases where this exposes the beneficial owner to the risk of becoming a victim of crime. In this regard, EU legislators must be criticised for the evident disregard of the protection obligations incumbent upon them. Data communication must be prohibited wherever there are indications of such risks. Legislators themselves have an obligation to rule out such a scenario and cannot delegate their protection responsibility to Member States.

What is more, to implement the necessary protection of fundamental rights by procedural means would require safeguards that go significantly beyond the wording of MLD 2018. The following provisions seem appropriate at the level of EU law: rules that require record keeping; the right to object to the communication of data; rules that lay down erasure obligations; a right to judicial oversight; provisions for an adequately effective system of sanctions that can act as a deterrent to prevent potential abuse. In addition, the data subjects should receive information on who has accessed their data. The disclosure requirement cannot be a one-way street and apply only to the beneficial owners included in the register, but not to those wanting to use the data for their own purposes. Exemptions from this are feasible for a limited transitional period, for example for ongoing journalistic investigations or NGOs.

The directive is a long way from these kinds of safeguards. EU legislators themselves must take action to remedy these shortcomings. Efforts in this direction, such as those implemented in German law that are reported on above,[404] are insufficient to close the gap. Irrespective of the ECJ's clear demands, it is also imperative from a legal policy perspective to ensure that data protection is guaranteed as a fundamental right at the level of EU law. Especially in the case of cross-border scenarios, there would otherwise be a risk that the lowest level of protection will ultimately prevail, thus failing to ensure adequate data protection as required by Art. 8 CFREU.

2. Public country-by-country reporting

The above criticism against making the transparency register publicly accessible can similarly be applied to the European Commission's initiative to make country-by-country reports, which have to date only been available to the participating tax authorities, available to the public. Here, too, there is a lack of adequate guarantees to ensure the required protection of personal data. There is a similar failure to recognise that the monitoring of tax compliance is first and foremost the responsibility of the tax authorities and that, because of their strict duty to uphold fundamental rights, they are the only institutions to provide adequate assurances that the information retrieved is not used for improper purposes.

However, there is another reason why the initiative is drawing criticism. As demonstrated above, the international exchange of information has been taken to new heights in terms of both quantity and quality in the past nearly three years.[405] Before the implementation deadlines – such as those for the requirement to notify cross-border tax planning – have passed and before experience has been gathered with the new legal instruments, it seems not only wrong in terms of legal policy, but also risky from an EU law perspective to introduce pCbCR and thus increase the existing level of interference to a significant extent. It may be helpful to refer to the ECJ's Schecke ruling: the Council and the Commission have to weigh up the affected interests of the European Union and the fundamental rights of the data subjects in a balanced manner before writing disclosure requirements into law.[406] This includes evaluating the existing instruments before new measures are resolved that exacerbate the interference.

3. Perspective of additive interference with fundamental rights

As demonstrated above, the current and especially the future design of the transparency register is in conflict with data protection requirements. The same applies to the European Commission's plans to develop country-by-country reporting into public country-by-country reporting. This means that the issue of additive interference with fundamental rights does not arise at present. This concept can only be used to explain that interference with fundamental rights that are legitimate when viewed in isolation can turn

404 See C.II.1.f) (p. 43) above.

405 See C.III.2.c) (p. 58) above.

406 ECJ, judgement of 9 November 2010 C-92/09 and C-93/09, C-92/09, C-93/09 (Schecke GbR) marginal note 79.

into a violation of such rights owing to their compounding effect. This means that additive interference with fundamental rights will only attain its own relevance when legitimate measures are assessed, which is exactly what is not happening in the present case.

However, if the transparency register is revamped in compliance with data protection requirements, it is not expected to cross the threshold to additive interference with fundamental rights, even when taking into account the exchange of information under tax law. If there is sufficient reason for public disclosure, holders of fundamental rights will in principle have to make concessions on their right to informational self-determination, even if other disclosure requirements under commercial and company law and the international exchange of information have already led to considerable interference with informational self-determination. There is not much point in abstract discussion of the issue, given that the severity of a measure – especially when considered in combination with other interferences with fundamental rights – always depends on its exact nature. All the more reason for legislators to focus on this perspective, because the severity of interference of existing disclosure and information requirements is already extremely high. It would be appropriate for responsible policy making to take this into account at the level of international standard setting in order to avoid the risk that the European Union and Germany assume obligations at that level without being able to turn them into binding legal norms.

E. Conclusions for legal policy

The results of this study were presented in the summary at the beginning of this document. The discussion below can therefore be limited to a summary assessment of the basic themes and central lines of development underlying the increase in disclosure requirements.

The debate reflects a new aspect of the age-old problem of conflicting social objectives. A balance has to be struck between freedom, security and fair distribution. The need to think about balancing these principles is attributable to a change in the security situation, where an effective fight against money laundering seems required not only to rein in organised crime, but also to combat terrorism. This is all the more relevant given the number of spectacular revelations by the Fourth Estate of hitherto unknown schemes for money laundering, tax evasion and damaging aggressive tax planning. Think of examples such as the Luxembourg leaks, the Panama and the Paradise papers.

The international community of nations has responded to these undesirable developments by introducing a large number of different measures. In the area of anti-money laundering, one example is the Financial Action Task Force (FATF), which has developed international standards to counter this problem. An important project in the area of tax is the BEPS initiative, which is aimed at countering damaging tax competition and unfair tax strategies of international companies; its recommendations have been incorporated into an action plan supported by a large number of countries. The international standards have since been adopted into EU as well as national law. Examples include in particular the transparency register (sections 18 ff. of the GwG) and the country-by-country report (section 138a of the AO).

The legitimacy in principle of the measures taken can hardly be called into question. In order to realise the area of freedom, security and justice (Art. 3 TEU), effective measures and instruments have to be in place to counter the threats of money laundering, terrorism financing and tax evasion. Even if there is expected to be consensus about the shortcomings and the need to correct them, we must at the same time emphatically recall that any tightening of social and economic control goes hand-in-hand with a loss of freedom.

It is of concern in this regard that the European Union has legislated beyond the extent of international standards, which make no provision for disclosure requirements such as those associated with the transparency register, which has already been implemented in EU law, and the pCbCR sought by the European Commission. It remains to be seen whether they are necessary to meet the set objectives. It is impossible to predict this need at present because the effectiveness of the existing set of instruments has not yet been assessed. In terms of legal policy, everything suggests therefore that we should not immediately rush into the second step before there is clarity about the effectiveness of the large number of measures already taken.

What can be criticised as inappropriate activism from a legal policy perspective may also have an underlying element in fundamental rights. From a data protection perspective, disclosure requirements are conceivably the most severe interference with the right to privacy. As soon as personal data is made public, the right to decide on how personal data can be used, which is guaranteed in the Charter of Fundamental Rights and the Basic Law of Germany, is almost completely denied. On publication, the holders of fundamental rights lose control of the data collected, as it can be copied, stored and combined with other data in almost limitless ways. Proven safeguards, such as erasure requirements and rights to information, have no effect.

As a matter of principle, responsibility for balancing the conflicting objectives mentioned above falls to politicians, who must also observe the constitutional requirements laid down by the Charter of Fundamental Rights and the Basic Law. Limitations of legislative freedom arise mainly on the basis of the proportionality principle and the concept of fundamental rights protection through organisation and procedures. If the right to informational self-determination is restricted on the basis of EU law, the data protection requirements must also be laid down at the level of EU law. Just how seriously they ought to be taken has been made clear in the ECJ's two most recent rulings on data retention. Although the Data Retention Directive pursues high-level objectives under EU law, such as the fight against terrorism, and the ECJ has recognised that data retention is useful in pursuing these objectives, the corresponding measures conflict with insurmountable data protection barriers.

The design of the transparency register set out in in the Fourth Money Laundering Directive fails to take adequate account of the requirements developed in the ECJ's recent case law, even from a procedural perspective. The need for a virtually public transparency register and the resulting over-reaching implementation of international standards on anti-money laundering have been insufficiently examined and explained. Substantive shortcomings are the absence of valid cause for the surveillance and the complete inadequacy of the protection mechanisms. This assessment applies all the more to the Fifth Money Laundering Directive of 2018, which intends to make the transparency register accessible to anyone. Germany should insist on amendments to this directive and implement the necessary safeguards in national law, at least for an interim period. Germany should not approve the pCbCR proposed by the European Commission.

Any reference to the transparency principle of EU law in an attempt to justify the extension of disclosure requirements, which has been criticised in this study, must be emphatically opposed. Although EU law recognises a transparency principle, its purpose is exclusively to oversee the actions of the European Union itself. If the general thrust of the transparency principle is disregarded, the idea of transparency will be turned from an instrument to rein in and supervise government power into a tool of social control. This would confirm the warnings raised in social philosophy, which predicted that the transparency society could inadvertently be turned into a control society. We should therefore think of the European Data Protection Supervisor's criticism of the transparency register as an emphatic reminder that it is not the responsibility of private players to ensure compliance with the legal system.

List of abbreviations

AEAO	Anwendungserlass zur Abgabenordnung (Fiscal Code Application Decree)
AG	Aktiengesellschaft (German stock corporation)
AG	Die Aktiengesellschaft (journal)
AG	Advocate General
AktG	Aktiengesetz (German Stock Corporation Act)
AnaCredit	Analytical credit datasets
AO	Abgabenordnung (Fiscal Code of Germany)
Art.	Article
ATA	Anti-tax avoidance
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority)
BayBO	Bayerische Bauordnung (Bavarian Construction Regulations)
BB	Der Betriebsberater (journal)
BBG	Bundesbeamtengesetz (Federal Civil Service Act)
BEPS	Base erosion and profit shifting
BGB	Bürgerliches Gesetzbuch (German Civil Code)
BGH	Bundesgerichtshof (Federal Court of Justice)
BGHZ	Sammlung der Entscheidungen des BGH in Zivilsachen (collection of Federal Court of Justice decisions in civil matters)
BImSchG	Bundes-Immissionsschutzgesetz (Federal Immission Control Act)
BKAG	Bundeskriminalamtgesetz (Federal Criminal Police Office Act)
BMF	Bundesministerium der Finanzen (Federal Ministry of Finance)
BRR	Business Register Regulation
BVerfG	Bundesverfassungsgericht (Federal Constitutional Court)
CbCR	Country-by-country reporting
CFREU	Charter of Fundamental Rights of the European Union
CR	Computer und Recht (journal)
CRS	Common Reporting Standard
CSR	Corporate social responsibility

DAC	Directive on Administrative Cooperation
DB	Der Betrieb (journal)
DStR	Deutsches Steuerrecht (journal)
DStRE	Deutsches Steuerrecht/Entscheidungsdienst (online database of decisions on German tax law)
EC	European Community
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
ed.	editor
EFG	Entscheidungen der Finanzgerichte (journal)
e.g.	exempli gratia (for example)
EntgTranspG	Entgelttransparenzgesetz (German Transparency in Wage Structures Act)
EStG	Einkommensteuergesetz (German Income Tax Act)
EU	European Union
EuGRZ	Zeitschrift für Europäische Grundrechte (journal)
EuZW	Zeitschrift für Europäisches Wirtschaftsrecht (journal)
EEC	European Economic Community
ECB	European Central Bank
FATF	Financial Action Task Force
ff.	and the following (pages or lines)
FG	Finanzgericht (German Fiscal Court)
FKAustG	Gesetz zum automatischen Austausch von Informationen über Finanzkonten in Steuersachen (German Financial Accounts Information Exchange Act)
fn.	footnote
G20	Group of Twenty (of the world's major advanced and emerging economies)
GDPR	General Data Protection Regulation
GewO	Gewerbeordnung (German Trade Regulation)
GG	Grundgesetz (Basic Law for the Federal Republic of Germany)
GmbH	Gesellschaft mit beschränkter Haftung (German limited liability company)

GmbH & Co. KG	Gesellschaft mit beschränkter Haftung und Compagnie Kommanditgesellschaft (limited partnership with the sole general partner being a limited liability company)
GmbHR	GmbH-Rundschau (journal)
GwG	Geldwäschegesetz (German Money Laundering Act)
HGB	Handelsgesetzbuch (German Commercial Code)
HRV	Handelsregisterverordnung (German Commercial Register Regulation)
ibid.	ibidem (as cited in the preceding item)
IFG	Informationsfreiheitsgesetz (German Freedom of Information Act)
IFRSs	International Financial Reporting Standards
IStR	Internationales Steuerrecht (journal)
KG	Kommanditgesellschaft (German limited partnership)
KGaA	Kommanditgesellschaft auf Aktien (German partnership limited by shares)
Lfg.	Lieferung (supplement)
LG	Landgericht (German Regional Court)
Ltd	Limited company
MAD	Market Abuse Directive
MLD	Money Laundering Directive
MMR	MultiMedia und Recht (journal)
NGO	Non-governmental organisation
NJW	Neue Juristische Wochenschrift (journal)
NLMR	Newsletter Menschenrechte (journal)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (journal)
NWB	Neue Wirtschafts-Briefe (journal)
NZG	Neue Zeitschrift für Gesellschaftsrecht (journal)
OECD	Organisation for Economic Co-operation and Development
OHG	Offene Handelsgesellschaft (German general partnership)
OLG	German Higher Regional Court
PublG	Publizitätsgesetz (German Public Disclosure Act)
RabelsZ	Rabels Zeitschrift für ausländisches und internationales Privatrecht (journal)
RAO	Reichsabgabenordnung (Reich Fiscal Code)

SGB	Sozialgesetzbuch (German Social Code)
SGb	Sozialgerichtsbarkeit (journal)
SMEs	Small and medium-sized enterprises
SWI	Steuer und Wirtschaft International (journal)
TEEC	Treaty establishing the European Economic Community
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TrEinV	Transparenzregistereinsichtnahmeverordnung (German Regulation on Inspection of the Transparency Register)
WM	Wertpapier-Mitteilungen (journal)
WpHG	Wertpapierhandelsgesetz (German Securities Trading Act)
WpPG	Wertpapierprospektgesetz (German Securities Prospectus Act)
ZfbF	Zeitschrift für betriebswirtschaftliche Forschung (journal)
ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht (journal)
ZHR	Zeitschrift für das Gesamte Handels- und Wirtschaftsrecht (journal)
ZIP	Zeitschrift für Wirtschaftsrecht (journal)
ZRP	Zeitschrift für Rechtspolitik (journal)
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft (journal)

Bibliography

Albers, Christel, in: Hübschmann/Hepp/Spitaler/Söhn, *Abgabenordnung, Finanzgerichtsordnung*, supplement 181, June 2004, section 30 of the AO.

Albrecht, Jan Philipp, "Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung", CR 2016, 88.

Bachmann, Gregor/Eidenmüller, Horst/Engert, Andreas/Fleischer, Holger/Schön, Wolfgang, *Rechtsregeln für die geschlossene Kapitalgesellschaft*, 2012.

Baum, Michael, "Datenschutz im Steuerverwaltungsverfahren ab dem 25.5.2018. Teil I: Unmittelbare Geltung der DSGVO und bereichsspezifische Regelungen in der AO", NWB 2017, 3143.

Baum, Michael, "Datenschutz im Steuerverwaltungsverfahren ab dem 25.5.2018. Teil II: Zulässigkeit der Verarbeitung personenbezogener Daten durch Finanzbehörden", NWB 2017, 3203.

Baum, Michael, "Datenschutz im Steuerverwaltungsverfahren ab dem 25.5.2018. Teil III: Informationspflichten der Finanzbehörden und Auskunftsrechte der betroffenen Personen", NWB 2017, 3143.

Baums, Theodor, "Zur Offenlegung von Vorstandsvergütungen", ZHR 169 (2005), 299.

Bayer, Walter/Habersack, Mathias (eds.), *Aktienrecht im Wandel*, volume I, 2007.

Bernsdorff, Norbert, in: *Charta der Grundrechte der Europäischen Union*, 3rd ed. 2014, Art. 8.

Britz, Gabriele, "Europäisierung des grundrechtlichen Datenschutzes?", EuGRZ 2009, 1.

Buck-Heeb, Petra, *Kapitalmarktrecht*, 9th ed. 2017.

Federal Ministry of Justice, *Handbuch der Rechtsförmlichkeit*, 3rd ed. 2008.

Cascante, Christian/Topf, Cornelia, "'Auf leisen Sohlen'? – Stakebuilding bei der börsennotierten AG", AG 2009, 53.

Czakert, Ernst, "Die gesetzliche Umsetzung des Common Reporting Standards in Deutschland", DStR 2015, 2697.

Di Fabio, Udo, in: Maunz/Dürig, *Grundgesetz*, supplement 39, July 2001, article 2 (1).

Drüen, Klaus-Dieter, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, supplement 133, August 2013, section 30 of the AO.

Dutt, Verena/Spengel, Christoph/Vay, Heiko, *Der EU-Vorschlag zum Country-by-Country Reporting im Internet – Kosten, Nutzen, Konsequenzen*, 2017.

Fleischer, Holger, "Corporate Social Responsibility", AG 2017, 509.

Frenzel, Eike, in: Paal/Pauly/Ernst/Frenzel/Gräber/Hennemann/Körffer/Martini/Nolden, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, 2nd ed. 2018, Art. 5 GDPR.

Fuchs, Ingo/Lakenberg, Thomas, "Das Transparenzregister nach dem neuen Geldwäschegesetz", NJW-Spezial 2017, 463.

Gebauer, Martin/Teichmann, Christoph (eds.), *Europäisches Privat- und Unternehmensrecht*, 2016.

Gurman, Olga, *Die Vorstandsvergütung nach der Finanzkrise*, 2018.

Hamacher, Rolfjosef, "Datenschutz und internationaler Informationsaustausch", IStR 2016, 171.

Han, Pyong-ch'ol, *Transparenzgesellschaft*, 2012.

Harbarth, Stephan/Freiherr von Plettenberg, Hanno, "Aktienrechtsnovelle 2016: Punktuelle Fortentwicklung des Aktienrechts", AG 2016, 145.

Held, Cornelius, *Intelligente Videoüberwachung*, 2014.

Hennrichs, Joachim, "Die Grundkonzeption der CSR-Berichterstattung und ausgewählte Problemfelder", *Zeitschrift für Unternehmens- und Gesellschaftsrecht* 2018, 206.

Hirte, Herbert, "Kommerzielle Nutzung des Handelsregisters", CR 1990, 631.

Hoffmann-Becking, Michael, "Rechtliche Anmerkungen zur Vorstands- und Aufsichtsratsvergütung", ZHR 169 (2005), 155.

Hommelhoff, Peter, "Europäisches Bilanzrecht im Aufbruch", RabelsZ 62 (1998), 381.

Hood, Christopher/Heald, David (eds.), *Transparency*, 2006.

Hopt, Klaus, in: Baumbach/Hopt, *Handelsgesetzbuch*, 38th ed. 2018.

Hornung, Gerrit, "Anmerkung zum Urteil des EuGH vom 9.11.2010 (C-92/09; C-93/09, MMR 2011, 122) – Datenschutz und Veröffentlichung von Empfängern von EU-Agrarsubventionen im Internet", MMR 2011, 127.

Jansen, Stephan A./Schröter, Eckhard/Stehr, Nico, *Transparenz*, 2010.

Jarass, Hans D./Pieroth, Bodo, *Grundgesetz für die Bundesrepublik Deutschland*, 4th ed. 2016.

Johlen, Heribert, in: Stern/Sachs, *Europäische Grundrechte-Charta, GrCh*, 2016, Art. 8 CFREU.

Jutzi, Thomas, *Unternehmenspublizität*, 2017.

Schmidt, Karsten, *Handelsrecht*, 6th ed. 2014.

Kaiser, Anna-Bettina, *Die Kommunikation der Verwaltung*, 2009.

Kaltenstein, Jens, "Kernfragen des 'additiven' Grundrechtseingriffs unter besonderer Berücksichtigung des Sozialrechts", SGb 2016, 365.

Kirchhof, Gregor, "Transparenzregisterdaten für jedermann?", ZRP 2017, 127.

Klöhn, Lars, "Das deutsche und europäische Insiderrecht nach dem Geltl-Urteil des EuGH", ZIP 2012, 1885.

Knieper, Rolf, *Eine ökonomische Analyse des Notariats*, 2010.

Kotzenberg, Jochen/Lorenz, Karsten, "Das Transparenzregister kommt", NJW 2017, 2433.

Kraft, Gerhard/Ditz, Xaver/Heider, Christian, "Internationaler Informationsaustausch", DB 2017, 2243.

Kühling, Jürgen, in: Pechstein/Nowak/Häde/Boysen*, Frankfurter Kommentar zu EUV, GRC und AEUV*, 2017, Art. 16 CFREU.

Kühling, Jürgen/Martini, Mario, "Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?", EuZW 2016, 448.

Kühling, Jürgen/Sackmann, Florian, "Datenschutzordnung 2018 – nach der Reform ist vor der Reform?!", NVwZ 2018, 681.

Langenbucher, Katja (ed.), *Europäisches Privat- und Wirtschaftsrecht*, 2017.

Lücke, Oliver, "Die Angemessenheit von Vorstandsbezügen – Der erste unbestimmbare unbestimmte Rechtsbegriff?", NZG 2005, 692.

Ludwigs, Markus, "Kooperativer Grundrechtsschutz zwischen EuGH, BVerfG und EGMR", EuGRZ 2014, 273.

Lutter, Marcus, "Die handelsrechtliche Publizität – direkt für die Mülltonne?", AG 1994, 363.

Luttermann, Claus/Großfeld, Bernhard, *Bilanzrecht*, 4th ed. 2005.

Meinzer, Markus, "Transparenzregisterdaten für jedermann?", ZRP 2017, 127.

Merkt, Hanno, *Unternehmenspublizität*, 2001.

Merkt, Hanno, "Das IFRS Conceptual Framework aus regelungsmethodischer Sicht", ZfbF 2014, 477.

Mertens, Hans-Joachim, "Anm. zur BVerfG-Entscheidung", AG 1994, 370.

Meyer-Ladewig, Jens/Nettesheim, Martin, in: Meyer-Ladewig/Nettesheim/von Raumer, *Europäische Menschenrechtskonvention*, 4th ed. 2017.

Michael, Lothar, *Der allgemeine Gleichheitssatz als Methodennorm komparativer Systeme*, 1997.

Müller, Nadja, "Das Geldwäscheregister nach Art. 30 und 31 der Vierten Geldwäscherichtlinie und seine Vereinbarkeit mit der Rechtsprechung des EuGH zur Vorratsdatenspeicherung", ZStW 2016, 1021.

Niederdorf, Jan, *Die Bedeutung des Steuergeheimnisses für die Tax Compliance – Eine vergleichende Betrachtung zwischen Schweden und Deutschland*, 2009.

Noack, Ulrich, "Online-Unternehmensregister in Deutschland und Europa", BB 2001, 1261.

OECD, *Action Plan on Base Erosion and Profit Shifting,* 2014.

OECD, *Transfer pricing documentation and country-by-country reporting*, 2015.

OECD, *Transfer Pricing Documentation and Country-by-Country Reporting, Action 13 - 2015 Final Report*, 2016.

OECD, *Standard for automatic exchange of financial account information in tax matters*, 2nd ed. 2017.

Oppel, Florian, "Internationaler Informationsaustausch in Steuersachen – Teil I", NWB, 359.

Pache, Eckhard, in: Pechstein/Nowak/Häde/Boysen, *Frankfurter Kommentar zu EUV, GRC und AEUV*, 2017, Art. 52 CFREU.

Petersen, Jens, *Unternehmenssteuerrecht und bewegliches System*, 1999.

Petruzzi, Raffaele/Navisotschnigg, Florian, in: Lang/Haunold, *Transparenz und Informationsaustausch*, 2017, p. 51.

Raiser, Thomas/Veil, Rüdiger, *Recht der Kapitalgesellschaften*, 6th ed. 2015.

Rösch, Franziska, *Zur Rechtsformenwahl des europäischen Gesetzgebers im Lichte des Verhältnismäßigkeitsgrundsatzes – von der Richtlinie zur Verordnung*, 2013.

Rüsken, Reinhart, in: Klein, *AO*, 13th ed. 2016, section 30.

Ruiner, Christoph/Schramm, Michael/Fischer, Thorsten, "Foreign Account Tax Compliance Act", DB 2011, 2403.

Schaub, Peter, "Das neue Transparenzregister naht – Überblick über die Regelungen und praktische Auswirkungen für Personenvereinigungen", DStR 2017, 1438.

Schenke, Ralf P., *Verfassungs- und europarechtliche Fragen des § 138a AO-Entwurf*, August 2007 (legal opinion: available at Lexinform 0208905).

Schenke, Ralf P., in: Stern/Becker, *Grundrechte-Kommentar*, 3rd ed. 2018, article 10 of the GG.

Schmidt, Karsten/Lutter, Marcus (eds.), *Aktiengesetz*, 2015.

Schmitt, Carl, *Die Diktatur*, 8th ed. 2015.

Schnitger, Arne/Brink, Thomas/Welling, Timo, "Die neue Meldepflicht für grenzüberschreitende Steuergestaltungen (Teil I)", IStR 2018, 513.

Schoch, Friedrich, *Informationsfreiheitsgesetz*, 2nd ed. 2016.

Scholz, Sebastian, *'Einheit der Gesellschaft' versus 'Vielheit der Gesellschafter'*, 2015.

Seer, Roman, in: Tipke/Kruse, *Abgabenordnung, Finanzgerichtsordnung*, supplement 145, July 2016, section 117 of the AO.

Seibert, Ulrich/Wedemann, Frauke, "Der Schutz der Privatanschrift im elektronischen Handels- und Unternehmensregister", GmbHR 2007, 17, (20).

Simons, Cornelius, "Corporate Social Responsibility und globales Wirtschaftsrecht", *Zeitschrift für Unternehmens- und Gesellschaftsrecht* 2018, 316.

Skouris, Vassilios, "Leitlinien der Rechtsprechung des EuGH zum Datenschutz", NVwZ 2016, 1359.

Specht, Louisa in: Sydow, *Europäische Datenschutzgrundverordnung*, 2nd ed. 2018, Art. 85.

Spindler, Gerald, "Das Gesetz über die Offenlegung von Vorstandsvergütungen – VorstOG", NZG 2005, 689.

Spindler, Gerald/Stilz, Eberhard (ed.), *Kommentar zum Aktiengesetz*, 2015.

Stein, Torsten, in: *Die Hochschullehrer der Juristischen Fakultät der Universität Heidelberg, Richterliche Rechtsfortbildung*, 1986, p. 619.

Stöber, Michael, "Anzeigepflichten in Bezug auf Steuergestaltungen im deutschen und europäischen Recht", BB 2018, 1559.

Teichmann, Christoph/Epe, Daniel, "Die neuen Meldepflichten für künftig erwerbbare Stimmrechte (§§ 25, 25a WpHG)", WM 2012, 1213 ff.

Veil, Winfried, "Die Datenschutz-Grundverordnung: des Kaisers neue Kleider", NVwZ 2018, 686.

Wakounig, Svetlana, in: Lang/Haunold, *Transparenz und Informationsaustausch*, 2017, p. 29.

Wartenburger, Lucas, in: Schön, *Rechnungslegung und Wettbewerbsschutz im deutschen und europäischen Recht*, 2009, p. 49.

Weber-Grellet, Heinrich, "Steuerrecht und Demokratie", ZRP 2014, 82.

Weismantel, Jan, *Das 'Recht auf Vergessenwerden' im Internet nach dem 'Google-Urteil' des EuGH*, 2017.

Wilburg, Walter, *Entwicklung eines beweglichen Systems im bürgerlichen Recht*, 1950.

Wöhrer, Viktoria, "Öffentliches Country-by-Country-Reporting verfassungswidrig", SWI 2017, 25.

Wolff, Heinrich Amadaeus, in: *Frankfurter Kommentar zu EUV, GRC und AEUV*, 2017, Art. 7 CFREU.

Würtenberger, Thomas, *Zeitgeist und Recht*, 2nd ed. 1991.

The Foundation for Family Businesses

Prinzregentenstrasse 50
80538 Munich
Germany

Phone + 49 (0) 89 / 12 76 400 02
Fax + 49 (0) 89 / 12 76 400 09
E-mail info@familienunternehmen.de

www.familienunternehmen.de

ISBN: 978-3-942467-67-4