Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part III

Consequences for the interpretation of the GDPR (and the Lawmaker's Room for Manoeuvre)

*Maximilian von Grafenstein**

There may be no other fundamental right of the European Charter of Fundamental Rights (ECFR) that raises more questions on the precise object and concept of protection than the right to data protection in Article 8 ECFR. A prominent example is the principle of purpose limitation. The preceding parts of this three-parted series has shown how this ambiguity creates various problems both on the conceptual level of fundamental rights as well as on the level of ordinary law (esp. the GDPR). However, it has also been shown how a re-connection of data protection law to concepts of risk regulation helps to clarify these ambiguities. On this basis, the third and last part of this series will draw several conclusions for the interpretation of the GDPR. In particular, this third part will focus on the following aspects: First, the actual room for maneuver of the EU legislator transposing the proposed concept for Article 8 ECFR into ordinary law (especially the GDPR). Second, the implications for interpreting the principle of purpose limitation with particular respect to the legal basis (Art. 5 sect. 1 lit. a and b and Art. 6 sect. 1 and 4 GDPR). Third, the phenomenon of the multitude of overlaying risk assessments, beginning with the assessment on an abstract-general basis conducted by the legislator to the variety of individual-specific risk assessments that the controllers and processors have to carry out (when applying the legal norms). Fourth, the possibility to make these risk assessments scale. The three-parted series will conclude with an outlook on further ambiguities to be clarified.

Keyboards: Article 8 ECFR | Fundamental Right to Data Protection | Precautionary Principle | Risk-Based Approach | GDPR | Regulating Risks | Effects on Public and Private Actors

I. Introduction: Controlling Risks Through (Not to) Article 8 ECFR Against the Other Fundamental Rights

The first part of this series has shown how an ambiguous object and concept of protection of the fundamental right to data protection, as enshrined under Article 8 ECFR, creates various fundamental problems both on the conceptual level of fundamental rights as well as on the level of ordinary law (especially of the GDPR).[1] Therefore, the preceding second part of this series elaborated on a refinement of the object and concept of the fundamental right to data protection in Article 8 ECFR by taking the various concepts of risk regulation into account. In do-

DOI: 10.21552/edpl/2021/3/6

* Maximilian von Grafenstein LL.M. is Professor for 'Digital Self-Determination' at the Berlin Career College of the University of the Arts in Berlin (UdK), part of the Einstein Center Digital Future (ECDF) as well as co-head of the research program Governance of Data-Driven Innovation at the Alexander von Humboldt Institute for Internet and Society. For correspondence: <max.grafenstein@hiig.de>.

1 See Max von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I: Finding an Appropriate Object and Concept of Protection by Re-Connecting Data Protection Law with Concepts of Risk Regulation' (2020) 6 EDPL 4, 509.

ing so, this contribution proposed to understand the so-called risk-based approach not as a control of risks *to* Article 8 ECFR but as a control of risks *through* Article 8 in favour of all other fundamental rights.[2] From this refined object and concept of protection on the level of fundamental rights, it is now possible to draw conclusions for the interpretation of the GDPR. In doing so, this third and final part of the series will focus on the following aspects: First, the actual room for maneuver of the EU legislator transposing the proposed concept for Article 8 ECFR into ordinary law (especially the GDPR). Second, the interpretation of the principle of purpose limitation with particular respect to the legal basis (Art. 5 sect. 1 lit. a and b and Art. 6 sect. 1 and 4 GDPR). Third, the multitude of overlaying risk assessments, beginning with the risk assessment on an abstract-general basis conducted by the legislator to the variety of individual-specific risk assessments that the controller and processor have to carry out (when applying the respective GDPR-provisions). And last but not least, the possibility to make all these risk assessments scale. This three-parted series concludes with an outlook on further ambiguities to be clarified in the next future.

II. Conclusions for the Legal System of the GDPR

Interestingly, while the object of protection of the fundamental right to data protection under Article 8 ECFR is (or has been) quite unclear, Article 1 sect. 2 of the GDPR leaves no doubt: 'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.' The question that this provision does not clarify is, of course, the interplay of Article 8 ECFR with the other fundamental rights. The reader may therefore again refer to the concept as proposed in this contribution. The next chapters will demonstrate how this helps answer several of the questions raised in the first part of this series. Each chapter will therefore start with one of these questions.

1. The Effects of Article 8 ECFR on Public and Private Parties

Before addressing these questions, it is worth shedding light on the general room of manoeuvre and interpretation when transposing the proposed object and concept of protection on the level of ordinary law. A particular question is in this regard: Does the right to data protection in Article 8 ECFR bind public and private actors equally?[3] Article 8 ECFR certainly binds public actors, but whether it has a direct effect on private actors, or only an indirect effect is disputed amongst scholars.[4] The ECJ has not yet decided this question, at least not explicitly, since all decisions were based on secondary law.[5] At least at the level of secondary law, the GDPR applies to both the private and public sector. However, clarity on the level of fundamental rights can, also in this respect, help to interpret the secondary law as well as the room for future manoeuvre of the legislator. For example, while Article 8 sect. 1 ECFR requires a legal basis for the personal data processing by public actors, this may not necessarily have to be the case for private actors.

a. Same Procedural Protection Measures Differently Applied (According to the Different Nature of Risks)

As shown in the second part, the approach of this contribution proposes to understand Article 8 ECFR as a protection of the data subject's autonomy against the risks caused by personal data processing and, in particular, that the processing does not undermine the data subjects' autonomous exercise of the (other) fundamental rights. To this aim, the right provides a set of instruments to control the processing risks to these more or less specific objects of protection. Therefore, while the instruments *per se* remain the same, the risks that arise in the private and public

2 See Max von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II Controlling Risks Through (not to) Article 8 ECFR Against Other Fundamental Rights' (2021) 7 EDPL 2, 190 - 205.

3 Cf. the interplay of the 'defensive' and 'protection function' of fundamental rights with respect to actions by private parties and the State, Max von Grafenstein, *The Principle of Purpose Limitation: The Risk-Based Approach, Legal Principles and Private Standards as Elements for Regulating Innovation* (Nomos, 2018) 109 et seq, with further references regarding the level of the ECHR, ECFR and German Basic Law.

4 See Matthias Niedobitek, 'Entwicklung und allgemeine Grundsätze' in Detlef Merten and Hans-Jürgen Papier (eds.), *Handbuch der Grundrechte in Deutschland und Europa – Band VI/1 „Europäische Grundrechte I'* (C F Müller, 2010) § 159, 103 with further references.

5 See (n 3).

sector can be different and, thus, the protection instruments may be applied differently as well.[6]

One fundamental difference between processing risks in the public and private sectors is the asymmetry of information power. For historical reasons, informational power asymmetry deserves special attention in the public sector, which a constitution can reflect by a guarantee called 'separation of *informational* power' [emphasis added].[7] A prominent example for a measure that safeguards such a 'separation of informational power' is, not surprisingly, the principle of purpose limitation.[8] At least in Germany, the principle of purpose limitation has been established to counterfeit an unlimited collection and processing of personal data by the State. On this basis, the principle of purpose limitation directly results from the principle of legal clarity. It ensures, first and foremost, that citizens are able to foresee the purposes for which the State is collecting the data, and public agencies and legal courts are able to interpret the law accordingly.[9] In contrast, the principle of legal clarity does not apply to the private sector, which in principle leaves more room for manoeuvre for processing personal data in the private sector than the public sector. Of course, the German right to informational self-determination is not a direct benchmark for the contribution here. Nevertheless, the idea of informational separation of powers can also be referred to in other legal regimes in which it is about limiting the State's use of power. Even if private companies today are accumulating enormous informational power and can, in fact, considerably limit the scope of action of other persons, these companies do not yet have such a comprehensive and integrated control and enforcement apparatus as the State.

Against this background, one may wonder why the legislator is actually allowed to specify broader purposes than a controller in the private sector. For example, on one hand, the EDPB requires a controller to make purposes like 'research', 'IT security' and 'marketing' more specific than just that.[10] On the other hand, almost the same wording in Articles 32 and 89 GDPR used by the legislator remains uncriticised. This is astonishing since the dynamics of development in the private market are even more challenging for private actors than for actors in the public sector, where a first framing of the processing purposes can be done along the tasks and competencies of public authorities, which are relatively static compared to the private sector. (By the way, this framing of processing purposes through the public tasks and competencies is the origin of the notion that processing purposes must be 'precisely specified for certain areas', which means certain areas of competencies of the respective public authority.[11])

However, there are two reasons that put this observation into perspective: First, as mentioned before, private actors can also accumulate (even enormous) informational power over data subjects. In such cases, the stricter requirements that usually apply only to the public actors, can apply accordingly to these powerful private actors.[12] 'Accordingly' because in such cases the principle of legal clarity still does not apply. However, given the comprehensive and deep insights into the data subjects' private life and the extremely high unspecific risk that this information could one day be misused, the protective measures may become as strict as in the public sector. A second reason for why the legislator may shape laws in an undetermined way as described can be regulatory-technical constraints.

b. Regulatory-Technical Constraints of Making a Law like the GDPR

An example for such a regulatory-technical constraint is when the legislator sets up rules for the processing of personal data for 'research', 'IT security' and 'marketing'. In these cases, the legislator does so (usually) not for its own purposes, e.g. for intelligence

6 (n 3), 547 et seq.

7 See, however, Pohle, who emphasizes the function of an 'informational separation of power' with respect all kinds of organisation, thus, also private organisations, Jörg Pohle, 'Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung' (Humboldt-Universität zu Berlin, 2018) 255.

8 See Evelien Brouwer, The forgotten purpose of purpose limitation, in Leonard Besselink et al (eds.), *The Eclipse of the Legality Principle in the European Union*, (Wolters Kluwer, 2011) 280 and 291 et seq; Nikolaus Forgó et al, *Zwecksetzung und informationelle Gewaltenteilung* (Nomos Verlag, 2006).

9 Cf. BVerfG, 13th June 2007, 1 BvR 1550/03 (Kontostammdatenabfrage – Retrieval of Banking Account Master Data), 71, 73 and 74.

10 See on the one hand, the EDPB's critical Opinion 03/0213 on purpose limitation, 2 April 2013, 00569/13/EN, WP 203, and on the other hand the same but uncriticized wording in Articles 32 and 89 GDPR, for instance.

11 Cf. the first Decision on Population Census of the German Constitutional Court, BVerfG, 15th of December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83, 179.

12 Cf. the German Constitutional Court in its recent decision from 6th November 2019, 1 BvR 16/13 (Right to be forgotten I), 88.

reasons, but to balance the conflicting rights in the private sector. The legislator must therefore provide for instruments that protect the data subjects against the risks arising in the private sector, while at the same time these protection measures must be proportionate regarding the controller's opposing fundamental rights. In such a situation, finding an appropriate solution depends mainly on the particularities of a specific context. Thus, if the legislator does not (perhaps it cannot) precisely specify the purpose on a general-abstract legal basis, one has to ask whether this requires further or complementary measures to effectively protect the data subject against the corresponding risk.[13] This can be the case if the legislator has not sufficient knowledge to regulate a certain matter in detail, for example, because the regulated area is too dynamic (e.g. in innovative fields) and the legislator does not yet know (and cannot yet foresee) all specific risks in its details.[14]

This means that if the EU legislator allows the processing of data for 'marketing' purposes in such a general term, the legislator may require the controller to provide further information (e.g. about its formalized knowledge on which its personalised advertising is based) to effectively protect the data subject. Similarly, if the legislator privileges the processing of data for 'research' purposes, the legislator may require the controller to assess the necessary additional measures on its own. This is also what Art. 24, 25 and 32, as well as 89 GDPR do: after the legislator has provided a first balancing of the conflicting rights, by establishing the legal basis for the processing in Art. 6 GDPR, they direct further balancing to the controller including the remaining assessment of the risks and appropriate protection measures.[15] The fact that the legislator hardly ever makes substantial balancing decisions on its own, but instead transfers this task to the controller (as well as to data subjects, data protection authorities and legal courts), is worthy of criticism.[16] However, a reason for this can be, as already said, that the legislator did not have sufficient knowledge about the actual risks in all imaginable contexts during the legislation process.

c. Sidenote: There is no 'General Prohibition Rule' for the Private Sector (but a Legal-Technical Constraint)

An interesting side note to this is that the GDPR does actually not implement a 'general prohibition rule' for data processing in the private sector simply because this was required by Article 8 sect. 2 ECFR.[17] While the separation of informational power may require a legal basis for each kind of personal data processing in the public sector, this is not necessarily the case in the private sector. In principle, in the private sector, the legislator could also require a certain legal basis only for specific risks, for example, the data subject's consent for the (first) publication of information about a data subject's personal life, while the processing of less personal information like a data subject's IP address to present her the website she is visiting may not require such a legal basis. However, since there may always be a situation where a controller should be able, for example, to publish personal information about a data subject also without her consent (e.g. for journalistic purposes), it is difficult to determine all these situations in advance. Thus, there is also the aforementioned regulatory-technical reason for the structure of Art. 6 sect. 1 GDPR: as long as the legislator does not (or cannot) clearly distinguish between situations where consent is required and those where it is not, it must require a legal basis for any kind of processing. The legal-technical reason for this is that the consent-requirement does only work if the processing is initially forbidden.[18] A first result from this situation is that the legislator must create *alternative* legal bases, such as for the 'legitimate interests', to enable the controller to process personal data also without the consent of

13 Cf. C Callies, Schutzpflichten, in: Detlef Merten / Hans-Jürgen Papier (eds.), Handbuch der Grundrechte in Deutschland und Europa – Band II „Grundrechte in Deutschland – Allgemeine Lehren I', Heidelberg: C. F. Müller, 2006, § 44.

14 See M von Grafenstein, 'Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design' in Gloria González-Fuster et al (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, Edward Elgar Publishing* (Edward Elgar Publishing, 2019), as part of their series Research Handbooks in Information Law.

15 See regarding the regulatory burden resulting from such a transfer of the risk assessment, the 1st part at point III. 2.

16 See, for example, the discussion between Bart van der Sloot and Raphaël Gellert in Bart van der Sloot, 'Ten Questions about Balancing' (2017) 3 EDPL 2, 187 - 194; Raphaël Gellert, 'On Risk, Balancing, and Data Protection: A Response to van der Sloot' (2017) 3 EDPL 2, 180-186; and Bart van der Sloot, 'Editorial' (2019) 5 EDPL 1, 1-9.

17 See in this regard, for instance, the Art. 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, pp. 14 et seq.

18 See in more detail (n 3) 553.

the data subject. A second consequence is that if the legislator does not determine the diversity of risks in its regulation itself, such as by providing a certain legal basis for a specific processing risk, one must take this diversity of risks into account when *interpreting* these provisions.

2. Legalising the Data Processing by Complying with the GDPR

This leads us to the question of how the proposed concept, in particular, for the specification of the purpose and for the purpose compatibility assessment can help clarify the GDPR-conformity of the data processing, with a special view to the required legal basis.

a. The Specification of the Purpose and the Appropriate Legal Basis According to the Risks to the Data Subject's Fundamental Rights

The first question raised in the first part of this series was how specific a controller must actually specify its processing purpose and, in doing so, whether the controller should specify the purpose from its own perspective or the data subject's point of view.[19] The proposed concept shows that it is neither a purely *subjective* perspective of one nor the other. Rather, the data subject's fundamental rights provide an *objective* scale: The controller must reveal the specific risks caused by its processing by specifying its purpose accordingly; and the data subject cannot refer to all kinds of interests or 'reasonable expectation' but only insofar as these are protected by their fundamental rights (and as often specified by ordinary law). However, subjective elements remain: just as it is about the data subject's fundamental (i.e. *subjective*) rights, it is the controller which sets *its purpose*. As it has been explained, the controller's purpose is a very useful element for the risk assessment because the purpose, i.e. what somebody *wants* to do, is a reliable indicator that determines with a sufficient degree of probability the causal link between the processing and harm to the data subject's rights. There are of course other, more objective indicators (e.g. the context of the processing and nature of the data).[20] However, since the purpose refers to the intention of the controller, it is particularly suited as a mechanism for the legal attribution of responsibility (before harm occurs). It is important to note in this regard that the processor cannot simply evade liability, for instance, by concealing the actual intended processing (with the actual risk involved) and by pretending a substantially different purpose that would lead to no risk or a lower risk. Nor can the controller escape liability on the basis of mere ignorance. This is because the law *requires* the controller to disclose the real risks to the fundamental rights of the data subjects by correctly specifying its purpose; and the controller is able to proactively fulfil this requirement because it can determine the risks on the basis of an objective scale by referring to the data subject's fundamental rights (and a data protection agency is able to retrospectively verify or falsify the results of this assessment conducted by the controller through referring to the context of the processing and/or nature of the data, and so on).

So let us apply this approach to ordinary law: Because the GDPR requires the controller to correctly indicate the risk by its purpose, the controller *must* do so in order to legalise its processing. If the controller does not correctly specify the purpose (ie. risk by its processing), the severity of this legal violation depends on the *actual* risk and the implemented measures (which may be assessed, as said previously, by referring to the context of the processing and nature of the data): If a controller does not correctly specify a risk by its purpose but does apply most other GDPR-requirements according to the *actual* risk, this incorrect specification conflicts with the principle of purpose limitation (Art. 5 sect. 1 lit. b GDPR) and, as a consequence from this, with the transparency principle (Art. 5 sect. 1 lit. a, further specified by Art. 12-15 GDPR). However, a wrongly specified purpose does not necessarily turn the data processing illegal as a whole.[21] This would only be the case if the processing, with its actual risk, cannot be based on a legal basis (Art. 6 sect. 1 GDPR). Insofar, the specific legal basis pre-structures – even if in a fairly abstract way – the balancing of opposing fundamental rights with respect to the interest

19 See 1st part at point I. 2.

20 Max von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II Controlling Risks Through (not to) Article 8 ECFR Against Other Fundamental Rights' (2021) 7 EDPL 2, 198.

21 Cf. the decision of SG Neuhausen from the 8th June 2021 (S 13 AS 1134/20), 38.

in the data processing and its respective risks. Compliance with (or better, the concrete implementation of) the other legal requirements then determines the extent of the risk that is to be legalised by the legal basis.

Article 6 sect. 1 GDPR provides for several ways in which this balancing exercise is or can be carried out: Either the data subject unilaterally consents to the risk (!) because she may consider the value of what she receives in exchange for her consent to be higher than the risk (lit. a); or the data subject and the controller agrees bilaterally to exchange the controller's efforts to fulfil the contract for the risk (!) that she incurs in the fulfilment of the contract (whereby both parties generally value what they receive higher than what they give, i.e. the data subject considers the *value of the controller's performance of the contract* to be higher than the processing risk for her, while the controller considers *the value of what it can do with the data* in relation to the contract to be higher than its efforts for performing the contract); or the legislator itself decides on which interests (e.g. of the controller, the public, or even the data subject) supersede what kind of processing risk (lit. c-e); or finally, it is up to the controller to carry out the balancing exercise by weighing its own interests (and of third parties and/or the public) against the processing risk to the data subject (lit. f). Thus, the controller can only legalise its processing operation through specifying (the risks caused by) its processing purpose correctly and by choosing the appropriate legal basis – given the implemented further measures.

b. Purpose Compatibility as a Pre-Assessment of Whether a Rebalancing of the Conflicting Fundamental Rights is Necessary

On the basis of the proposed concept it is also possible to systematize the criteria as proposed by the EDPB for the compatibility assessment and as it is now almost literally established in Art. 6 sect. 4 GDPR. As criticized in the first part of this series, the set of criteria does lead to any result, at least as long as each of them does not have an objective legal scale.[22] However, the approach proposed in this paper enables one to refine and systematize them. The reason is that the full set of fundamental rights of the data subject determines not only how a controller must specify its purpose correctly but also the 'context' of collection, the 'type of data', the 'distance' between old and new purposes, the 'impact' on the data subject, and on this basis, the 'additional safeguards'. For example, data is transferred from one context into another one if the processing causes a specific risk to another object of protection than before (e.g. personal data has been processed in an employment context for payroll purposes, with respect to Article 15 ECFR, and is later used in a judicial tax fraud case, which is covered by Article 47 ECFR). In the same way, one can measure the impact on data subjects and the distance between purposes (e.g. the distance is smaller if the new purpose reveals just a higher risk for the same object of protection as concerned before than if the new purpose reveals a new risk to another object of protection). Similarly, the variety of all fundamental rights can determine the type of data (e.g. data about one's intimate behaviour or in his private or social sphere pursuant to Article 7 ECFR, or data revealing sex, race, colour etc. on the grounds of Article 21 ECFR, or data about the behaviour of an employee again in respect to Article 15 ECFR). And last but not least, all fundamental rights can help determine the appropriate safeguards to protect their respective legal guarantee.[23] The fact that all the criteria can and must be further determined by referring to the data subject's fundamental rights does not mean that they are useless. To the contrary, the criteria provide a useful set of analytical instruments for the risk assessment: Even if all criteria may be determined in the light of a same object of protection that is specifically concerned, they can shed light on another concerned aspect of this right. Thus, the criteria are useful to carve out the normative particularities of the specific case.

There is another aspect that should be clarified in relation to these criteria. In its Opinion, the EDPB proposed as a further criterion the 'reasonable expectations' of the data subjects,[24] which do not re-appear in Art. 6 sect. 4 GDPR.[25] The reason for the disappearance is that this additional criterion was actually unnecessary because the compatibility assessment requires the controller to compare the new processing purpose with the original purpose anyway. Since the

22 See Section I. 2.

23 See Section III. 2. C.

24 See EDPB, Opinion 03/2013 on Purpose Limitation, 24.

25 However, see recital 50 sent. 6 GDPR.

controller is not only required to specify its purpose but also make it explicit to the data subject (Art. 5 sect. 1 lit. b GDPR), this explicit purpose frames the data subject's reasonable expectations.[26] In view of the explicit original purpose, the data subject thus knows what to expect. By comparing the new and old purposes, the controller therefore already assesses the data subject's reasonable expectations, even if only implicitly.[27]

Last but not least, another question in the introduction of this series was whether the purpose compatibility assessment (Art. 5 sect. 1 lit. b and Art. 6 sect. 4 GDPR) and the legal basis (Art. 5 sect. 1 lit. a, which is further specified by Art. 6 sect. 1 GDPR) are two cumulative or alternative requirements. While the Art. 29 Data Protection Working Group considers both requirements as cumulative,[28] several scholars argue on the basis of different grounds that both requirements should be seen as alternative to each other.[29] Interestingly, following the concept in this contribution, both requirements are neither cumulative nor alternative, but build on and complement each other. The reason for this is that the compatibility assessment under the GDPR primarily requires the controller to assess whether its new purpose requires a new legal basis or not: If the new purpose does not cause a new risk (and hence constitutes just a 'formal' purpose change),[30] the new purpose is doubtlessly compatible with the original purpose and can be based on the same legal basis as the original purpose (cf. recital 50 sent. 2 GDPR). In contrast, if the new purpose causes a new risk to the data subjects' rights and the controller does not (or cannot) reduce this new risk to the original state, there is a *substantially* new purpose and the controller needs to re-assess the (perhaps another) appropriate legal basis, which *re*-balances the now differently opposing fundamental rights.[31] In this regard, it is worth to emphasize: in this re-balancing exercise, the term 'new risk' means a risk that *adds* to the old risk that resulted from the original purpose (either because the new purpose causes a higher risk for the same object of protection as concerned before or because the new purpose now causes an additional risk to another object of protection).[32] As already explained, whether there is a new risk that *adds* to the previous one is decisive because the data subjects may not have given their consent or not have concluded the contract or, simply, not used the service if they had known that this would lead to this new later risk. This missed opportunity for the data subject to avoid the collection of the data as a whole has to be considered in the re-balancing exercise.[33] Thus, the controller has to assess whether there is a legal basis on which such a new risk can be justified.

Against this background, it becomes clear why the purpose compatibility test and the requirement of a legal basis are complementary, or at least cumulative, rather than alternative requirements. The reason for this is that the second approach (i.e. alternatively of both requirements) implies that a legal basis could substitute a purpose compatibility assessment even if it comes to the result that the purposes are definitely incompatible. However, as has been shown, this is conceptually impossible. Rather, the controller must assess with respect to an appropriate (potentially new) legal basis whether its interest in the processing still outweighs the new risk (that adds to the previous risk resulting from the original purpose). If there is a new risk, the controller has to-reassess the legal basis (with respect to the implementation of additional safeguards). If the controller finds a legal basis, on which its interests still outweigh the new risks, the purposes are 'not incompatible'. But if the controller does not find such a legal basis, the new purpose is definitely incompatible.[34]

Thus, also in regards to the compatibility assessment, Article 6 sect. 1 GDPR provides for several ways

26 See in more detail the analysis of this 'framing' function of the purpose with respect to the case law of the ECtHR regarding Article 8 ECHR, (n 3) 351 et seq.

27 See also why this criterion is not very robust anyway, for instance, (n 3) 211 et seq.

28 See Art. 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 36 - 37.

29 See Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (2016) 49-50; S Assion, J Nolte and W Veil, *Commentary on the GDPR*, (Bundesanzeiger Verlag, 2017) Art. 6, 201-216.

30 See 2nd part of this series at point III. 2. b.

31 'Re-balance', because a first balancing of the conflicting rights has already been carried out with respect to the original purpose.

32 See 2nd part of this series at point III. 2. b.

33 This cutting off of the data subject's original behavioural alternatives is what Assion, Veil and Nolte are obviously overlooking when they advocate the application of the hypothetical collection test that the German Constitutional Court has developed regarding those situations where the data subjects originally had *no* behavioral alternatives, S Assion, J Nolte and W Veil, *Commentary on the GDPR* (Bundesanzeiger Verlag, 2017) Art. 6, 201-216.

34 See the differences between the terms, Art. 29 Data Protection Working Party, *O*pinion on purpose limitation, 21; and in more detail, (n 3) 579 et seq.

in which this balancing exercise is or can be carried out: Either the data subject unilaterally consents to the *new* risk because she may consider the value of what she receives in exchange for her consent to be higher than the *new* risk (lit. a); or the data subject and the controller agree bilaterally to exchange the controller's efforts to fulfil the contract for the *new* risk that she incurs in the fulfilment of the contract (whereby both parties generally value what they receive higher than what they give, i.e. the data subject considers the value of the controller's performance of the contract to be higher than the new processing risk for them, while the controller considers the value of what it can do with the data in relation to the contract to be higher than its efforts for performing the contract); or the legislator itself decides on which interests (e.g. of the controller, the public, or even the data subject) supersede what kind of *new* processing risk (lit. c-e); or finally, it is again up to the controller to carry out the re-balancing exercise weighing its own interests (and of third parties and/or the public) against the *new* risk to the data subject (lit. f). Also in this regard, the controller can only legalise its processing operation through specifying the *new* (risks caused by its) processing purpose correctly and choosing the appropriate legal basis, as well as implementing the necessary measures.

c. Spotlight on the Role of Risks in the Data Subject's Consent and the 'Legitimate Interests'-clause

On this basis, it is worth highlighting the implications of the proposed approach in particular for the 'legitimate interests'-clause and the consent of data subjects. Regarding the first, an interesting question is how one may actually differentiate between the purpose of the processing and the interest in the processing, as mentioned under Art. 6 sect. 1 lit. f GDPR. The EDPB sees the difference in the fact that the ''purpose' is the specific reason why the data are processed', while an interest 'is the broader stake'.[35] At first sight, this distinction is plausible. However, at a second look, one starts to ask for its added value for the balancing exercise? In contrast, on the basis of the proposed approach in this contribution, the essential difference between both terms is that the controller's interests can be captured through the lense of the controller's fundamental rights, while the purpose must be specified in view of the data subject's rights.[36] In my opinion, this distinction between both terms makes more sense because it fits well with the balancing exercise to be carried out under the 'legitimate interests'-clause when weighing the opposing rights.

Also for the actual balancing of the opposing rights, the proposed approach can help, at least, by giving it a more consistent structure. The criteria proposed by the EDPB suffer from the same ambiguity as the criteria for the compatibility assessment. This is no wonder, as they are almost the same: In essence, the EDPB refers to the impact of the processing on the data subject, the nature of the data, the way data are being processed, the data subject's reasonable expectations, the status of the data subject and the controller, the measures that the controller has taken to comply with its general obligations from the GDPR, as well as further measures.[37] Also in this context, the variety of the data subject's fundamental rights can help determine the proposed criteria for Art. 6 sect. 1 lit. f GDPR. The main difference to the compatibility assessment therefore is that the 'legitimate interests'-clause does not compare old and new risks (by referring to the original and the new purpose) but only to the risks that are caused by the current purpose.

The fewer risks the current purpose causes for the data subject's fundamental rights, the less these risks may override the interests of the controller (and third parties and/or the public). In my opinion, unspecific risks *per se* do usually not outweigh any legitimate interest in the processing, and also specific risks or even harm to the right to private life are often not overriding the interests in the processing as long as they remain under a certain threshold of relevance (which is exceeded, however, in the case of extensive profiles of data subjects). Further, as shown in the second part of this series, protection measures play an important role to reduce risks, such as a risk to privacy. With respect to the risks to the autonomous exercise of the data subject's other rights, the protection measures equally play a decisive role. If these measures effectively safeguard the autonomous ex-

35 See EDPB, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 96/46/EC, 24.

36 See (n 3) 316 et seq.

37 See Art. 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 36 et seq.

ercise of fundamental rights, there is little risk that can actually override the interests in the processing. Thus, all in all, elaborating more precisely on such specific risks opens much more room for maneuver under Art. 6 sect. 1 lit. f GDPR than has been done before. Of course, how this looks in detail is open for discussion.

With respect to the consent of data subjects, some authors seem to think that a purpose, which is specified in a too broad way, invalidates the consent altogether.[38] Contrary to this opinion, the proposed approach makes clear that such a consent is not invalid in its entirety, but can only legalise the processing insofar as its actual risk has been specified in the consent. Thus, if the controller specifies its purpose broadly in a consent and does not (or only superficially) indicate a specific risk to a fundamental right, the controller cannot refer to this consent if its processing *de facto* causes such a specific risk (for instance, to the data subject's autonomous exercise of the freedom to find an occupation).[39] Of course, the question of whether a purpose specified in a consent does not clearly indicate a specific risk to one or more fundamental rights also depends on the concrete context.[40] In some cases, a data subject can infer from the specific situation (and her general knowledge) what specific risk such an imprecise purpose implies. However, such doubts can quickly speak against the controller (more precisely, how the controller might want to use the data). In particular, if the consent – or, equally, a contract pursuant to Art. 6 sect. 1 lit. b GDPR – is considered a 'consumer contract term' in the meaning of the Directive 93/13/EEC on unfair terms in consumer contracts, 'the interpretation most favourable to the consumer shall prevail' (Art. 5). This means, for instance, that if a controller simply states in a consent to process the data for 'marketing', 'product innovation' or 'future research', such broad purposes cannot *per se* legalise specific risks to the data subjects' fundamental rights. The reason for this is that marketing, product innovation and future research can be carried out with anonymized data. Thus, these purposes do not necessarily require the processing of data to reveal aspects of the private life of the data subjects, to treat them in a particular way or impair their fundamental rights.[41] Thus, if the controller wants to be sure that it is allowed to process the data also in such a 'risky' way, the controller should make it clear in its consent form that is presented to the data subject. A contrary example might be the purpose of 'personalised advertising' that may sufficiently imply, from the data subject's point of view, that the controller processes the data to create profiles in regards to their personal interests (i.e. a risk to their right to private life) and uses this information to influence their purchasing decision (i.e. a risk to their private autonomy). The reason for this is that personalised advertising necessarily builds on profiling and must therefore be expected by the data subjects. Also in this regard, of course, the details are open for discussion.

In any case, understanding specific risks to the rights of data subjects as the *actual* object of their consent and thus not personal data *per se*, is crucial also for further implications in civil law. Many people seem to think, for instance, that data subjects exchange 'their data' against a data-driven service or product from the controller.[42] In reality, to the contrary, data subjects exchange a data-driven service or product against a specific risk to one or more of their fundamental rights. This is fundamentally different.

3. Data Protection by Design (Individual-Specific Risk-Assessments Adding to the General-Abstract Ones, Pursuant to Article 25 GDPR)

Given the preceding arguments, some readers may already have the following question in their mind: Does the proposed concept of Article 8 ECFR as a protection against processing risks mean that the so-called risk-based approach under the GDPR is not limited to the single provisions that explicitly men-

38 See Nikolaus Forgó et al, *The Principle of Purpose Limitation and Big Data* (Springer, 2017) 27/28; See also in the German literature, for example Jürgen Kühling and Benedikt Buchner, 'Datenschutz-Grundverordnung/BDSG' (C.H. Beck, 2018), Art. 4 Nr. 11,7, Art. 6, 179, Art. 7, 62; See also: Sebastien Schulz *Datenschutz-Grundverordnung* (C.H. Beck, 2018) Art. 6 Rn. 24; Stefan Ernst, *Die Einwilligung nach der Datenschutzgrundverordnung - Anmerkungen zur Definition nach Art. 4 Nr. 11 DS-GVO*, (2017) 7 ZD 3, 110-113; Stefan Ernst, *Datenschutz-Grundverordnung* (C.H., 2018) Art. 4, 78.

39 See the example (n 3) 35 et seq. and 636 et seq.

40 See again Art. 29 Data Protection Working Party, Opinion on the principle of purpose limitation, 16, 19, 21 etc.

41 See the examples for specific risks above under point III.2.a.i.

42 See, instead of many others: Eric Tjong Tjin Tai, 'Data ownership and consumer protection' (2018) 7 Journal of European Consumer and Market Law 4, 136–140. Ultimately, this is also relevant with regard to the new Consumer Directive.

tion it, but actually underlies the whole GDPR-protection system? The answer is: yes.[43]

a. Risk Assessments by the Legislator and the Controller

Let us start to explain this step-by-step: Article 1 sect. 2 GDPR makes it fairly clear that this law protects not only the fundamental right to data protection in Article 8 ECFR but actually all fundamental rights. On the level of ordinary law the object of protection is therefore clear. So, is there any reason to assume that the GDPR does not protect these fundamental rights against the *risks of personal data processing*? Do only those provisions in the GDPR protect these fundamental rights against processing risks, which explicitly mention the term 'risks'? I find this assertion disheartening. If this is the case, against what do then the other provisions protect the data subjects' fundamental rights? At least I see no other reason for protection. In my opinion, anyone who makes the contrary claim, i.e. that the risk-based approach applies only where it is explicitly mentioned, should explain this in more detail. Of course, one may ask the question why the GDPR mentions the term 'risks' only in these few provisions. But the answer to this question is not difficult to give, it only requires to contextualise this norm within the broader legal system:

First of all, one should recall the basic difference between law-making on a general-abstract level and applying a general-abstract law in an individual-specific case.[44] On this basis, it gets clearer that the *entire* GDPR protects the fundamental rights of the data subjects against risks, however, on a *general-abstract* level. The GDPR-legislator made its own risk assessment on this general-abstract level aiming with each provision (from the definition of the scope in Article 2 GDPR to the processing principles in Article 5 up to the remedies and sanctions in Articles 77 et seq. GDPR) at controlling risks to fundamental rights caused by the processing of personal data. In contrast, the provisions that *explicitly* refer to risks require that the controller (and to some extent the processor) also carry out such risk assessments, but now in respect to its individual-specific case – and here comes the astonishing aspect that may be worthy of criticism: with respect to all other GDPR-provisions. Of course, one can criticize this legislative order in view of the remarkable regulatory burden it places on the addressees of the regulation. We discussed this problem in the preceding parts of this series. However, the wording in the GDPR is clear.

b. The Interplay of Article 25 with Article 5 and All the Rest of the Rules

On this basis, one can determine further layers oscillating between such general-abstract and individual-specific risk assessments. A first step to do so is to focus on the data processing principles listed under Article 5 GDPR, which are explicitly mentioned in Article 25 GDPR, and which the controller must implement into the technical and organisational design. From a regulatory viewpoint, legal principles are not only applicable universally[45] but also serve as a regulatory objective that leave the regulation addressee sufficient leeway in order to take the particularities of its specific context into account and to find the optimal solution. In contrast, conditional if-then-sentences, i.e. 'legal rules', dictate exactly the controller what it has to do and, therefore, are more rigid but also provide for higher legal certainty.[46] While the effects and appropriateness of both instruments have been discussed in more detail with respect to innovation in another contribution,[47] this paper focuses on the interplay between these two risk regulation instruments: By combining both instruments, the

43 See also Raphael Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk- Based Approaches to Data Protection' (2016) 4 European Data Protection Law Review 2, 481-292.

44 This difference is what Quelle might overlook when she considers 'an inevitable clash between the risk-based approach and obligations which are not risk-oriented', The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too, Tilburg Law School Legal Studies Research paper Series No. 17/2017, esp. on p. 19.

45 See Raphael Gellert, 'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk- Based Approaches to Data Protection' (2016) 4 European Data Protection Law Review 2, 481-292.

46 Focusing on privacy-related principles, Winston Maxwell, 'Principles-based regulation of personal data: the case of 'fair processing'' (2015) 5 International Data Privacy Law 3, 212 to 214. Claudio Franzius, 'Modalitäten und Wirkungsfaktoren der Steuerung durch Recht', in Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann and Andreas Voßkuhle (eds.), *Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation*' (C.H. Beck, 2012) § 4, 7.

47 See Max von Grafenstein, 'Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the 'state of the art' of data protection-by-design' in Gloria González-Fuster et al (eds.), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics* (Edward Elgar Publishing, forthcoming).

GDPR-legislator apparently aims at bringing the 'best of both worlds together'. On the one hand, the GDPR provides processing principles with its universally applicable objectives. On the other hand, the GDPR provides a set of legal rules that dictate, more or less, what to do exactly under certain circumstances – 'more or less', because these legal rules are again peppered with broad legal terms, such as the terms of 'risk' and 'purpose'. Given the combination of both instruments, a controller must therefore take the overarching principles into account when the rules do not sufficiently address the need for protection (measures) or are not sufficiently precise. To give an example of the transparency principle established under Article 5 sect. 1 lit. a alt. 3 GDPR, which is further specified by the legal rules in Articles 12 et seq. GDPR: While these rules mainly specify *what* the controller has to do, the transparency principle dictates *how* it must implement these rules (i.e. in an optimal way given the specific circumstances)[48] – and as far as the specific rules do not apply, the controller must furtherly assess whether additional transparency measures are needed to optimally meet the overarching aim to protect the data subject against the respective risks through transparency measures. What Article 25 GDPR now adds to this is that the controller must *effectively* implement all these principles and legal rules by appropriate technical-organisational measures on the basis of an individual-specific risk-assessment.

c. Sidenote on the Overlapping Risk-Assessments

Against this whole concept of protection (i.e. including the level of fundamental rights and of ordinary law), it gets clear why an 'assessment of the risks to the other rights', according to Article 25 GDPR, and an 'assessment of the impact on the processing', pursuant to Article 35 GDPR, is just at first glance contradictory.[49] The simple reason for this is that the scopes of application of Article 8 ECFR and the other fundamental rights overlap. The conclusion of the legal scholar Gellert that compliance with data protection law 'signals' a violation of the other fundamental rights is, therefore, correct, in principle. However, it is not just some signal that would hint only to unspecific risks in the background somewhere. Rather, the controller must comply with data protection law, i.e. apply the appropriate data protection measures, to control in particular specific risks to one or even more of the other fundamental rights. In this legal system, implementing the processing principles plays a crucial role because it *mediates* the risks to the other fundamental rights: Implementing the principles and, in their light, the legal rules through the appropriate technical and organisational measures, the controller can reduce the likelihood and severity not only of unspecific risks but also of the specific risks to the fundamental rights.[50]

4. Increasing Degree of Formalization of Risk-Assessments (and the Possibility to Make it Scale)

Looking at the many overlapping (specific) risk assessments, it can be argued that this creates quite a regulatory burden. In fact, this is a severe problem of ordinary data protection law, especially of the GDPR[51] – which is, doubtlessly, improvable. Some readers may particularly argue whether it is useful to understand the purpose limitation principle in the proposed way, as it adds just another risk assessment to all the other ones. Just to give an overview:

The first risk assessment starts with the definition of the scope. Already here, taking the other fundamental rights into account helps clarify the scope of application, especially by referring to the content, purpose, and result element: The content element applies when data contains information that reveals aspects about a data subject's private life. This criterion therefore defines the scope of Article 8 ECFR with respect to Article 7 ECFR. In contrast, the result criterion defines the scope of Article 8 ECFR in regards to the other fundamental rights. The other rights thus determine what result is legally relevant or, in con-

48 See Franzius, (n 45) 7.

49 See Raphael Gellert, 'Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing' (2017) Trends and Communities of legal informatics: IRIS 2017 - Proceedings of the 20th International Legal Informatics Symposium, 527 532; and already before him, Claudia Quelle, 'The data protection impact assessment, or: how the General Data Protection Regulation may still come to foster ethically responsible data processing' (2015).

50 See in more detail how this methodology works in practice at Max von Grafenstein, 'How to build data-driven innovation projects at large with data protection by design' (2020) HIIG Discussion Paper Series, 72 et seq.

51 See Winfried Veil, 'The GDPR: The Emperor's New Clothes: On the Structural Shortcomings of Both the Old and the New Data Protection Law' (2019) Neue Zeitschrift für Verwaltungsrecht, 686 et seq.

trast, must be socially accepted by the data subject. Finally, the purpose-criterion can be seen as the criterion, which defines the scope of Article 8 ECFR most independently of other rights: the mere intention of the controller 'to evaluate, treat in a certain way or influence the status or behaviour of an individual' opens the scope of Article 8 ECFR, even if a controller does not aim to process data in a way that reveals aspects about a data subject's private life or causes a specific risk against another fundamental right. The mere intention is sufficient, as a 'reasonable ground' for granting precautionary protection. Interestingly, by adopting these three criteria from the EDPB, the ECJ applies the approach proposed here, at least, insofar as it orientates the application of Article 8 ECFR *also* toward the other rights.[52]

In any case, looking at the purpose element, one may even pose the question of why it should be necessary to specify the purpose again when it has already been necessary to define the scope?

The situation is even worse: Even after the controller has (again) specified the purpose by taking the variety of all rights of the data subject into account, the risk assessment-exercise goes further if it wants to base its processing on the 'legitimate interests'-clause according to Art. 6 sect. 1 lit. f GDPR. This is why Morel and Prins propose to skip the next-following assessment, which is necessary if the controller should process the data for another purpose than specified before.[53] However, what Morel and Prins overlook is that the compatibility assessment is just the necessary pre-assessment to find out whether an additional legal basis for the new purpose is actually needed; this means that if the compatibility assessment leads to the result that there is no new risk, there is no need for the 'legitimate interests'-clause – which makes the whole assessment easier for the controller than if Moerel's and Prins' approach applied. The reason for this is that if there is no new risk, the controller does not have to additionally take the legitimate interests into account, what Morel and Prins require.

In any case, if the controller is an honourable woman and has done what the law requires, the next risk assessments is already awaiting her: the data protection by design-assessment in Article 25 GDPR – as well as the security assessment in Article 32 GDPR – and they should not overlook Article 24! But that is not all. The real assessment is right in front of us: the Data Protection Impact Assessment according to Art. 35 GDPR with its pre-assessment in sect. 1, possibly followed by reviews, consultations, and so on. Last but not least, we should not forget a substantial change of purpose, because if this happens, it will start all over again.

It is difficult to make sense of this multitude of overlapping risk assessments. However, there is some reason in it: Each assessment has its own special focus; and all assessments build on each other, with their increasing degree of formality. All of the overlapping risk assessments therefore serve as a layered system of protection, which becomes more formalized and rigid the more specific and higher the risk is.[54] One can see such an increasing formalization of requirements as the counterpart for the increasing risk that results from the controller's increasing informational power by its data processing.[55] This may comfort some readers as it seems to be fair. In any case, understanding the GDPR as a set of (more or less) overlapping risk assessments has the potential to make it scale, at least to some extent.

To avoid the impression that the previous sentence was only meant ironically, it is necessary highlighting the fact that Articles 40 to 43 GDPR foresee the possibility to standardise parts of the risk assessments, which indeed makes it scale. The reason for this is that the adherence to codes of conduct and certification mechanisms, as foreseen under Article 40 to 43 GDPR, reduces the legal uncertainty and transaction costs that controllers face when conducting the multitude of risk assessments. The entry point for this again is the proposed understanding of the principle of purpose limitation, as the following argumentation line may illustrate: First, codes of conduct and certification mechanisms must refer to processing operations; second, a controller must define these operations through specifying the processing

52 See ECJ C-434/16, 34 and 35, as well as EDPB, Opinion 4/2007 on the concept of personal data, 20 June 2007, 01248/07/EN, WP 136, 11.

53 See Lokke Moerel and Corien Prins, Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (2016) SSRN Electronic Journal, 49-50.

54 Max von Grafenstein, (n 3) 598 et seq.

55 Cf. in more detail regarding the problem of formalisation (e.g. through organisation, automation etc.) Jörg Pohle, 'Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung Berlin' (2018) <https://edoc.hu-berlin.de/bitstream/handle/18452/19886/dissertation_pohle_joerg.pdf?sequence=4&isAllowed=y> 246 et seq.

purpose; third, by specifying its processing purpose, the controller conducts its first risk assessment (actually the second one, after it has already determined the scope). Thus, on the basis of Articles 40 to 43 GDPR, the controller can standardise an essential part of this and all the following risk assessments, which more or less build on each other. This is often overlooked by scholars who discuss the question on how to implement the purpose limitation principle in technology.[56] The legal scholar Koops notes, for instance, that the 'enforcement of a legal norm (by means of technology) is problematic if the norm itself is complex due to openness, fuzziness, contextual complexity, or regulatory turbulence [words added in brackets by the author].'[57] Indeed, the purpose limitation principle is a complex and open norm. However, what Koops overlooks is the organisational level, where it is possible to break and narrow down the norm (i.e. specify and standardise the principle) to a granular level where it can even technically be standardised, which is the necessary prerequisite for a regulation by technology. This fact is of utmost importance to make the data protection by design-approach under Article 25 GDPR work.

Indeed, such *legal* standards for processing purposes must not be exclusive. This means that a controller is not obliged to adhere to such a standardised purpose but can also specify its purpose on its own (assess purpose compatibility, and determine the appropriate protection measures), in particular, if its purpose should be innovative and has thus not yet been standardised before: Of course, then, the controller is again faced with the higher legal uncertainty and transaction costs.[58] In any case, these considerations should have made clear that Article 40 to 43 GDPR provide, in principle, the necessary mechanisms so that the application of the GDPR can indeed scale.

56 See Bert Jaap Koops, 'The (in)flexibility of techno-regulation and the case of purpose-binding' (2011) 5 Legisprudence 2, 171-194; See also, as well as the master thesis by Z R Kostadinova, 'Purpose limitation under the GDPR: can Article 6(4) be automated?, Tilburg University.

57 See B-J Koops, ibid, p. 172; see already the discussion in the 70ies, for example, J Kilian, *Juristische Entscheidung und Elektronische Datenverarbeitung - Methodenorientierte Vorstudie*, Frankfurt a.M. 1974.

58 Cf. also the proposed case-study approach for assessing the effects of standardised purposes on innovation processes taking the (rough) examples of 'personalised marketing', 'statistical research' and 'scoring in an employment context'. See, (n 3) 624 et seq.

III. Outlook: Further Conceptual Ambiguities to be clarified

In a nutshell, the preceding considerations have shown that Article 8 ECFR, as well as the GDPR, protects data subjects against the risk that personal data processing undermines the autonomous exercise of their other fundamental rights. Understanding data protection law as a protection against such risks reaches back to the origins of the data protection and privacy debates. Ironically, the conceptual output of these debates waned at about the same time that risk regulation research began to take off, so it is not surprising that the conceptual results on regulating risks have not yet been sufficiently considered in the data protection and privacy discussions. Luckily, Article 8 ECFR brought back some movement into the debate, which I took as an occasion to re-connect data protection law with meanwhile well-known concepts of risk regulation. On this basis, it is possible to refine the concept of data protection law according to various regulation strategies, reaching from the harm-based to the risk-based approach up to the precautionary principle. Of course, the aim of this paper is not to impose these concepts *stante pede* on data protection law but to clarify the concepts behind the terms to assess, more precisely than before, the different normative elements, in particular, of the new fundamental right to data protection in Article 8 ECFR.

On this basis, it is possible to carve out that the actual reason and (legal) threshold of such data protection risk protection is the informational power asymmetry caused by personal data processing. This reason is an important first step to restrict the ever increasing scope of data protection law that supersedes all other fundamental rights, since not all informational power asymmetries are caused by the processing of personal data and can therefore be addressed by the applicable other fundamental rights alone. However, even if data protection law applies, a second important step to refine the broad and vague scope of data protection law is to see that not each processing causes the same risk to data subjects. Rather, more (data) protection is needed and required only the more informational power is accumulated and the more specific risks become against one or more of the data subjects' other fundamental rights. Finally, in respect to the subjective nature of Article 8 ECFR, it is important to note that data protection

law does not protect each arbitrary interest of data subjects in 'their' data but only such interests that are covered by their fundamental rights (which are often further specified by ordinary laws). Thus, data subjects do not have a right to control personal data *per se*, as if it were 'their property', but only a right to control the risks of the processing of data that relate to them. This is fundamentally different.

This result allows us to ask what we could do better in view of such a refined object and concept of protection of the fundamental right to data protection?

First and foremost, the ECJ should elaborate in much more detail and more precisely on the object and concept of Article 8 ECFR, in particular, with respect to the other fundamental rights. Even if the Court made some progress in determining the interplay of Article 7 and Article 8,[59] and also refers more and more to further fundamental rights,[60] the interplay still remains vague. This becomes obvious if one looks at the *Nowak vs Ireland* case: whether the claimant has access to comments of an examiner was, at the level of fundamental rights, less a question of the claimant's right to private life, to which the Court referred. Of course, the examiner's comments were also 'about' the claimant. However, the fact that an examiner evaluates the candidate's exam is quite irrelevant from a privacy perspective.[61] At least, such an evaluation should fit quite accurately with the candidate's 'reasonable expectations'. Instead, the normative focus of this case lies on the question of whether the data processing bears the risk to undermine the claimant's right to education under Article 14 ECFR, maybe with respect to the right to choose an occupation in Article 15 (if the exam in question was a final exam). In my opinion, this was not the case, irrespective of whether or not the other fundamental rights require such an access right. The reason for this is that Article 8 ECFR protects data subjects against the risks of the processing to their other fundamental rights. But in the *Nowak vs Ireland* case, there was no such processing-caused risk. The examiner did not use an algorithmic evaluation tool, nor did the risk result from the permanent and systematic storage of the data; thus, there was no special informational power asymmetry that has been caused by the processing, and which could not sufficiently (early) be addressed by the right to education. Thus, if the ECJ elaborated more precisely on the concept and interplay of Article 8 ECFR with regard to the other fundamental rights, it would be easier to come to nuanced and appropriate decisions – this applies not least to the legislator's work.

With respect to the lawmaking, many critics (also myself) have criticised the legislator for its uncreative approach that simply adopted the 'good old', generally known principles of data protection laws.[62] However, this paper has also illustrated that at least one of these principles, i.e. the principle of purpose limitation, is not so easily changed and even less easily abandoned, given the knowledge uncertainties regarding risks. To the contrary, the somewhat counterintuitive result of this contribution is that the purpose limitation principle is a highly appropriate regulation instrument to monitor, discover and control the risks caused by data processing against the data subject's autonomy, which can be further specified by all their other fundamental rights. What the legislator could do better is to specify which specific fundamental right referred to under Article 1 sect. 2 GDPR, such as to privacy or freedom or equality, typically requires which protection measures. The legislator cannot pass on every risk assessment to the addressees of its regulation, but must carry it out itself, provided it has the necessary context-specific knowledge. For some areas, such as marketing, this knowledge has long been available, so that the legislator could specify protection even more.[63] The legislator may also streamline the multitude of overlaying risk assessments to reduce the legislative risk of a disproportionate (because unnecessarily burdensome) protection. Further, the legislator must see the problem of the ever increasing scope of data protection laws

59 See ECJ-C 131/12, cip. 36-38 (Gonzalez vs Google Spain); ECJ-C 293/12 and C-594/12 (Digital Rights vs Ireland), 27 et seq.

60 See ECJ C-465/00, C-138/01 and C-139/01 (ORF vs Rechnungshof), cip. 74 and 89, focusing on the negative impact on the data subject to find another job; regarding Art. 11 ECFR, ECJ C-293/12 and C-594/12 (Digital Rights vs Ireland), 28, and even more extensively in ECJ C-203/15 und C-698/15 (Tele2 vs Sweden), 100 and 112; and regarding Article 47 ECFR, ECJ C-362/14 (Schrems vs Facebook), 95.

61 See, however, ECJ C-434/16, 57.

62 (n 50) 686-696; Max von Grafenstein, 'Interview mit Jan Philipp Albrecht' <https://www.hiig.de/datenschutz-fit-fuer-das-digitale-zeitalter-jan-phillip-albrecht-im-interview/> accessed 1 October 2021; As well as the analysis of this interview by Jürge Pohle, 'Dekonstruktion eines Rededuells' <https://www.hiig.de/dekonstruktion-eines-rededuells/> accessed 1 October 2021.

63 However, see now Article 21 GDPR, which is, at least, more specific than the corresponding provisions in the former Data Protection Directive.

in our (increasingly) digitised society. The right to data protection under Article 8 ECFR makes sure that the processing of personal data does not undermine the data subjects' autonomous exercise of her other fundamental rights, but its aim is not to supersede the normative extent and limits of the other rights. Thus, the legislator of secondary data protection law should make sure that the data subjects' rights do not undermine the limits of their other fundamental rights. This was the problem in the case YS and others vs Netherlands, where the Court sought to exclude the application of data protection law in order to avoid the claiming data subject's access to documents, which he would not have had on the basis of his right to good administration, according to Article 41 ECFR.[64] Similarly, the legislator should focus more clearly on the particular risks that are caused by the informational power asymmetries on the basis of the data processing, and not protect the data subjects against each kind of data processing *per se*.

However, controllers, processors and data protection authorities should also recognise that most of the aforementioned issues are solvable, more or less, by interpreting the GDPR accordingly (with the exception, for instance, of the extensive right to data access and, partly, information duties). The most important finding is in this regard that most legal terms within the GDPR are instrumental. This means that they make little sense if one tries to apply them to a specific case without an objective, substantive-normative scale at hand. Without such an objective substantive-normative scale, it is impossible to reliably assess (at least, I do not see another way) the content, purpose and result-elements for defining the scope of protection, how detailed a controller must specify its purpose, the difference between purposes and interests, as well as legal responsibilities with respect to purposes and means, further, the context of data collection, the distance between old and new purposes, the impact of the data processing on the data subjects, the appropriateness of data protection instruments and, last but least, the risks of data processing. Thus, actually, everything of data protection law! This paper has addressed several of these issues on the basis of the proposed re-fined object and concept of protection. However, it is possible to solve further questions as well, such as to further define the scope of protection,[65] or to assign the legal responsibilities to control the risks effectively.[66] In any case, if one has an objective and normative scale, such as the variety of all fundamental rights of data subjects (as specified by ordinary laws), all these regulatory elements can serve as useful tools to address the processing risks arising in specific contexts. Since most of these instruments are either broad legal terms or legal principles, controllers and processors may use their significant room for manoeuvre by specifying and standardising them. Such a proactive approach on the basis of Art. 40 et seq. GDPR does indeed have the potential to turn the GDPR's basic openness toward innovation into a competitive advantage.[67]

Last but not least, the question remains as to what the data subjects could do? Well, as long as the controllers specify their purposes as they stand and do not say anything about specific risk (or even hide such risks), data subjects will always prefer a concrete advantage (e.g. a free service) to an abstract processing risk.[68] However, such an unspecified (i.e. unspecific) risk does not mean harm to the data subjects – because such harm, or also a specific risk, requires a purpose compatibility assessment and, correspondingly, a new legal basis, new protection measures, and so on. In contrast, as soon as the controller really informs the data subjects about specific risks that the processing causes against one or even more of their fundamental rights, they should take this warning seriously. However, at the moment a specific risk is present, data subjects are able to properly balance concrete advantages against specific risks, finally.

64 See ECJ C -141/12 and C-372/12, 46.

65 For a first and rough approach in this direction, see Max von Grafenstein, (n 3) 532 et seq.

66 ibid 542 et seq.

67 See Max von Grafenstein, 'Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design, in Gloria González-Fuster et al (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar Publishing, forthcoming).

68 For this psychological heuristic rule see, Barry Sopher and Arnav Sheth, 'A Deeper Look at Hyperbolic Discounting' in Mohammed Abdellaoui et al, 'Uncertainty and Risk - Mental, formal, experimental representations' (Springer, 2007); For the privacy paradox, see Spyros Kokolakis, 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon' (2017) Computers & Security 64, 122-134.