D. Empirical approach in order to assist answering open legal questions

The preceding analysis highlighted, from time to time, which aspects cannot be answered by legal research alone.[1673] In summary, these aspects concern, in particular, the following questions: Under which conditions does the processing of personal data lead to a risk against an abstract constitutional position, such as democracy or solidarity?; in which cases is the individual typically not able to autonomously decide at all?; or how should data controllers specify the individual's decision-making process in order to enable them to effectively and efficiently manage the risks caused by the processing?; and finally, how must the corresponding mechanisms of regulated self-regulation be designed enabling data controllers to turn the specification of these requirements into a competitive advantage?

In order to answer these questions, it is necessary to collaborate with researchers from other research disciplines, using their theoretical concepts and methodological research designs. While researchers from social sciences may assist in assessing the risks caused by data processing and the appropriate protection instruments, researchers from economics may assist in examining the effects of the protection instruments on innovation processes.[1674] This chapter first illustrates different risk assessment methodologies, and focuses, subsequently, on the multiple-case study approach that appears to be best suited to bridge the research regarding the risks caused by innovation with research on the effects of risk protection instruments on innovation processes. Finally, the chapter concludes with a draft on how this methodology could be applied to the examples given in the

1673 See, in particular, above under point C. I. 1. c) Interim conclusion: Interdisciplinary research on the precise object and concept of protection,C. II. 3. b) aa) (3) (a) Research on the individual's decision making process (consent), C. II. 3. b) cc) (3) Articles 7 and/or 8 ECFR: Information pursuant to insights into personality and possibilities of manipulation, C. IV. 3. c) Conclusion: Specifying the decision-making process (Art. 24 and 25 GDPR).

1674 Cf. above under point A. II. 2. The regulator's perspective, B. I. Innovation and Entrepreneurship, B. II. Data protection as a risk regulation.

introduction of this thesis. In this regard, the idea of standardizing "purposes" of data processing will be discussed, in particular.

I. Clarifying different risk assessment methodologies

In order to illustrate different risk assessment methodologies, it is useful to differentiate between the object of the assessment and the methods applied for the assessment. This differentiation helps obtain a clearer picture about how different methods may be chosen or combined in order to assess the risks for a certain object of the risk assessment.

1. Different objects of risk assessments

Clarifying the object of a risk assessment assists, in particular, to differentiate between several assessments foreseen in data protection laws. For example, the General Data Protection Regulation foresees in its Article 35 the so-called data protection impact assessment. This assessment also refers to the risks caused by the processing of personal data, just as the requirement to specify the purpose and to limit the later data processing to this purpose, under Article 5 sect. 1 lit. b of the regulation. Thus, what is the difference between these two risk assessment methodologies?

a) Risk-based approach of purpose specification and limitation (Art. 5 sect. 1 lit. b GDPR)

As proposed in this doctoral thesis, the principle of purpose limitation consists of two components: The first component is the requirement to specify the purpose of the data processing. The function of this requirement is to discover specific risks caused by the data processing against the individual's fundamental rights to privacy, freedom and non-discrimination. The second component requires the data controller not to process personal data in way that is incompatible with the initial purpose. The function of this requirement is to control the risks caused by the later data processing compared to the risk originally specified. Thus, again, what is, in light of this approach, the difference between this kind of risk assess-

ment and the data protection impact assessment, pursuant to Article 35 of the General Data Protection Regulation?

b) Data Protection Impact Assessment (Art. 35 GDPR)

The first difference is that the data protection impact assessment constitutes a formalized procedure for the risk assessment. Article 35 sect. 1 of the General Data Protection Regulation states: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks." Section 3 provides three examples where a data protection impact assessment is required, in particular: First, with respect to an especially extensive form of profiling; second, in regard to processing of sensitive personal data; and third, with respect to a systematic monitoring of publicly accessible on a large scale. If this pre-assessment leads to the result that the data processing intended causes a high risk for the individual's fundamental rights, the controller is required to conduct a formalized impact assessment as specified in section 7 of Article 35. In this regard, pursuant to section 9, the controller shall also "seek the view of data subjects concerned or their representatives on the intended data processing". The regulation does not specify how these views shall be sought. However, if this formalized assessment affirms that there indeed is a high risk against the individuals' fundamental rights, the data controller must consult (again pursuant to a formalized procedure) the data protection authority, whose function is to safeguard that the high risk caused by the intended data processing is mitigated, pursuant to Article 36 of the regulation. Finally, section 11 of Article 35 of the regulation requires the controller to repeat the assessment, at least, if it changes the original purpose of the processing.

In light of these formalized requirements, the German White Paper on the Data Protection Impact Assessment correctly stresses the importance

of clarifying what this assessment substantively refers to.[1675] This question shall first be answered with respect to the principle of purpose limitation as established under Article 5 sect. 1 lit. b of the regulation. The German White Paper also provides guidance in this regard. It stresses that the data protection impact assessment refers, in essence, to the risk that personal data is processed in way that goes *beyond* the purpose specified by the controller. It considers that this might be the case because the data is processed by unauthorized third parties but also if the data is used, internally, in the data controller's organization in an illegitimate way. In light of this, the White Paper proposes to concentrate, elaborating on a methodology for the data protection impact assessment, on assessing the underlying motives that may exist on behalf of other departments in the data controller's organization and, in particular, the access to processing procedures and the personal data itself by public security agencies, competing private companies or research institutes.[1676] The White Paper therefore recommends to take, in particular, the following aspects into account in order to assess the risk that data protection rules might not be applied: First, the motivation of the organisation to change the purpose in an illegitimate way; second, the operative possibilities and opportunities within the organisation to illegitimately change the purpose; third, processing of personal data in third countries with a potentially lower level of protection (e.g. control mechanisms and judicial remedy); and fourth, the level of IT protection measures with particular respect to resolution mechanisms for conflicts between IT security (on behalf of business processes) and operative implementation of the individual's data protection rights.[1677]

In conclusion, the data protection impact assessment established under Articles 35 to 36 of the General Data Protection Regulation requires a formalized procedure for the assessment of risks that go beyond the purpose compatibility assessment. While Article 5 sect. 1 lit. b of the regulation requires the data controller to specify the purpose of the data processing with respect to the risks against the individual's fundamental rights, and to constantly control the later risks caused by the later data processing, this "first order" risk assessment however does not tackle the broader risk that the data controller may not appropriately apply these requirements. Against this broader ("second order") risk, the Data Protection Impact As-

1675 See Forum Privatheit, White Paper – Data Protection Impact Assessment, p. 29.
1676 See Forum Privatheit, ibid., p. 23.
1677 Cf. Forum Privatheit, ibid., p. 35.

sessment provides for a three layered regime of protection: First, a formalized procedure for the risk assessment; second, the data controller's duty to consult the data protection authority if the formalized assessment discovers a high risk; and third, by special fines applicable, pursuant to Article 83 sect. 4 lit. a of the regulation, if the data controller does not comply with the first two requirements.

c) Further methodologies (technology assessment and surveillance impact assessment)

Indeed, both risk assessments refer "only" to the fundamental rights of individuals concerned by the data processing. However, as stressed before, there can equally be risks caused by the processing of personal data against further aspects that may, from a social point of view, be relevant, such as abstract constitutional positions. Those abstract constitutional positions might be concerned by the data processing, in particular, with respect to the principle of democracy and the social state principle.[1678] The German White Paper differentiates, in this regard, the data protection impact assessment as required by Article 35 of the regulation from scientific assessments, such as technology assessments. These assessment methodologies particularly seek to reveal risks that are not yet known before and also refer to further aspects such as justice, as well as costs or public security.[1679] Similarly, Wright, Friedewald and Gellert give an overview about the so-called Surveillance Impact Assessment, which was developed in the SAPIENT project and consists in an advanced risk assessment methodology. This methodology seeks to address "not only issues of privacy and data protection, but also ethical, social, economic, and political issues."[1680]

1678 See above under point C. I. 1. b) bb) (2) A first review: decomposing the object and concept of protection, as well as B. III. 1. The individual's autonomy and the private/public dichotomy.

1679 See Forum Privatheit, ibid., p. 30, referring to Finn, R. L.; Wright, D.; Friedewald, M. (2013): Seven types of privacy. In: Gutwirth, S.; Leenes, R. et al. (ed.): European Data Protection: Coming of Age. Dordrecht: Springer, pp. 3 to 32, as well as Wright, D.; Kroener, I.; Friedewald, M. et al. (2014). A guide to surveillance impact assessment — How to identify and prioritise for treatment risks arising from surveillance systems. Deliverable 4.4. SAPIENT Project.

1680 See Wright, Friedewald and Gellert, Developing and testing a surveillance impact assessment methodology, p. 40.

However, in this regard, it shall be stressed, again, that it essentially depends on how the object and concept of data protection is defined, whether issues concerning the society as a whole, such as of individuality or solidarity, are covered by data protection or not.[1681] Correspondingly, Wright, Friedewald and Gellert recognize themselves that "both privacy and data protection are not only fundamental rights but are also highly complex concepts around which public opinion is diverse, fluid and often tied to other issues".[1682] It is, thus, the main challenge of interdisciplinary research to find out what is the object and concept of data protection. In any case, it can be helpful to involve the stakeholders concerned by data processing in order to clarify, at least, the concept of protection.[1683]

In conclusion, both risk assessments, i.e. the assessment inherent in the principle of purpose limitation and the data protection impact assessment under Article 35 of the regulation, refer to the individuals' fundamental rights and freedoms. However, the General Data Protection Regulation states, in its Article 1 sect. 2, to protect the individuals' fundamental rights and freedoms, beside their right to data protection. In this regard, thus, it is up to legal research in order to determine whether: the principle of purpose limitation and the data protection impact assessment only directly covers the individual's fundamental rights to privacy, freedom and non-discrimination; or whether it, indirectly, by taking a broader interpretation of the fundamental right to data protection, covers further aspects such as democracy and solidarity. Indeed, this thesis focuses on data protection instruments protecting the individual against risks against his or her specific fundamental rights. Which abstract constitutional positions precisely are protected by the fundamental right to data protection and which mechanisms come into question in order to protect these positions might be examined, in more detail, in other works.

1681 See above under point C. I. 1. b) bb) (2) A first review: decomposing the object and concept of protection, as well as B. III. 1. The individual's autonomy and the private/public dichotomy.

1682 See above under point C. I. 1. b) bb) (2) A first review: decomposing the object and concept of protection, as well as B. III. 1. The individual's autonomy and the private/public dichotomy.

1683 See Wright, Friedewald and Gellert, ibid., pp. 47 and 48.

2. Different assessment methods

This leads to the different methods coming into question in order to carry out a risk assessment. In Germany, the legal scholar Roßnagel examines such means, by focusing on technology assessments as a legal research discipline. His considerations refer to totally unknown risks against regulatory aims, and it can hence be argued whether or not this approach also applies to the risk assessment as proposed for the principle of purpose limitation, as well as the data protection impact assessment required under the General Data Protection Regulation. However, Roßnagel's considerations help, in any case, to get a clearer picture about the methods that can be applied, in principle, to any risk assessment. In particular, this approach is interesting because it examines how and by which means technological development can be influenced in such a way that it does not hinder but rather enables regulatory aims. Thus, comparable to the approach of the "regulation of innovation", as applied in this thesis, technology assessments as a research discipline shall also provide scientific evidence for regulatory decisions.[1684]

Indeed, Roßnagel stresses, similar to Voßkuhle's opinion illustrated in the introduction of this thesis, that the empirical results do not necessarily bind the lawyers assessing whether the technology complies with the law or not. There are two reasons for this cautious attitude: First, the public or the individuals concerned may under-estimate the risks and, therefore, praise the technology even if they are risky. And second, it is possible that the technology assessment does not provide for consistent results. This inconsistency must not be used as an argument against protection. Instead, here again, it then depends on the law to decide on whether it provides protection against such uncertain risks or not.[1685] However, coming to the means being appropriate for a technology assessment, Roßnagel gives an overview by describing, in particular, the following methods: Case studies, theories from social sciences, and expert and stakeholder participation.

1684 See Roßnagel, Technology assessment as a legal research discipline, p. 98.

1685 See Roßnagel, ibid., pp. 267 to 269; cf. already above under point C. II. 3. c) Interim conclusion: Fundamental rights determining the appropriateness of protection.

a) Examining abstract constitutional positions from a social science perspective

Roßnagel stresses that case studies may be particularly useful in order to describe the effects on the particular individual who uses a technology – but not on society as a whole. The reason for this failure is that they cannot describe, *per se*, the cumulative and synergetic effects of the usage of technology by several individuals. Indeed, Roßnagel does not neglect the value of case studies *per se*. Instead, he makes clear that without further theories from the social sciences it is impossible to draw conclusions from these specific cases to society as a whole. For such conclusions, it is necessary to interpret the results of the case studies in light of more general theories developed in research disciplines such as of communication psychology or communication sociology, and developmental psychology, which focus on the interdependencies between technology, individuals, and the society.[1686] These social research disciplines may ground their theories, in turn, on empirical research providing the data basis either as a bottom line for their hypothesis or for verifying their hypothesis.[1687] In any case, the moment causal relationships or (at least) correlations between socio-technological conditions and certain consequences are discovered, legal research can transpose these findings to its own research in order to assess whether these consequences and, thus, the conditions conflict with the regulatory aims, and how to react to it.[1688] These considerations are highly relevant with respect to abstract constitutional positions, such as democracy and solidarity that might be covered by data protection as a fundamental right.[1689] In order to find out whether data processing really threatens those values or not and, if so, how to reduce or even avoid such a threat, it is thus necessary to tightly work together with these social science research disciplines.

1686 See Roßnagel, ibid., pp. 176 and 177.

1687 Cf. Baxter and Jack, Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers, pp. 544 and 545; Eisenhardt and Graebner, Theory Building From Cases: Opportunities and Challenges, p. 25.

1688 Cf. Roßnagel, ibid., p. 181.

1689 See above under point C. I. 1. b) bb) (2) A first review: decomposing the object and concept of protection.

b) Pre-structuring interests through multiple-stakeholder and expert participation

Another method consists in the participation of stakeholders concerned by the use of a technology and expert groups. For gathering this kind of practice knowledge, Roßnagel lists four reasons: First, certain consequences of the use of certain technologies can only be foreseen on the basis of the practice knowledge from all stakeholders concerned; in this regard, it is often a question of political powers of whether all interests of the stakeholders concerned are covered in the solution finding process. Second, an answer to the question of whether or not the use of a technology results into a risk also depends on the subjective perception of the stakeholders concerned. Third, the use of a technology affects, usually, these stakeholders, differently. If not all interests of the stakeholders concerned are represented, it is hardly possible to fairly balance conflicting interests. Finally, the participation of all stakeholders concerned increases their willingness to accept the result of the technology assessment. In order to avoid these procedural risks or, vice versa, guarantee the success of the technology assessment, Roßnagel refers to the following iterative process: After a first examination of the current state of the art reported in literature, it is helpful to discuss this analysis with experts from the various interest groups concerned. On this basis, the technology assessment has to be refined, and this result must be discussed again. This process can be repeated until most conflicts or misconceptions are eliminated. In order to achieve this aim, it is recommended to also inform the public about the ongoing assessment and to take its feedback into account.[1690] In conclusion, multi stakeholder workshops may be a suitable means in order to pre-structure not only the divergent interests, but also the risks resulting from these interests and the protection instrument that balance best this conflict of interest.

c) Specifying 'decision-making process' by user-centered development of data protection-by-design

With particular respect to the possibilities to regulate technologies, Roßnagel highlights that information and communication technologies are

1690 See Roßnagel, ibid., pp. 182 to 185.

particularly suitable for a regulation by design. A regulation by design means that legal requirements can be implemented into the technology itself. Thus, with a particular view to information and communication technologies, there is no 'yes' or 'no' of being compliant with the law but, instead, there are several possibilities to adjust the technology in a way that meets the regulatory aim. In order to avoid paternalizing end users of these technologies, Roßnagel stresses that their interest should particularly be respected. Furthermore, information and communication technologies are particularly suitable for an iterative process of implementing legal requirements into their technological design. The reason is that these technologies are already being developed, mainly, by applying these iterative methods.[1691] Thus, the development of these technologies allows, in particular, an interactive and iterative process with risk assessment methodologies. Roßnagel highlights, indeed, an important aspect: as further these development processes get, the more difficult it becomes to implement legal requirements into the technological design.[1692]

Correspondingly, Margraf and Pfeiffer, two engineering scholars for IT security, advocate involving end-users of these technologies as early as possible into the technological development process. Giving the example of IT security, both authors stress the bad usability of those measures as one of the essential problems for achieving the regulatory aim.[1693] In order to illustrate the challenges related to usable security measures, they give the following specific example of encryption technologies: In an empirical study, end users of email services were asked to implement an email encryption technology. In order to function properly, this technology requires an end-user to generate a public and a private key. The users must send the public key to their communication partners enabling them to encrypt their emails designated for the user, and to verify the authenticity of the encrypted emails that the users send to them. In turn, the private key enables users to decrypt the emails that they receive from their communication partners, and to generate the code that is necessary for the verification of the email's authenticity. Amongst 12 end-users of this study, three users have sent their private key and seven users have used the public key in or-

1691 Cf. above under point A. I. 4. a) Coming from a practical observation: Startups and non-linear innovation processes.

1692 See Roßnagel, ibid., pp. 182 to 185.

1693 See Margraf and Pfeiffer, User-centric development for the Internet of Things, p. 246.

der to encrypt their emails: nobody was able to fulfill all of the required tasks. The encryption technology missed its aim totally.[1694]

Margraf and Pfeiffer conclude from this study that the main challenge for the success of security measures is to implement these measures in a way that does not overcharge the user of the technology. Referring to Saltzer and Schroeder, the authors stress one essential principle for the usability of privacy- and security-by-design: The so-called psychological acceptability principle. This principle contains two elements. The first element requires a user-interface that is easy to use. The second element requires that the internal mechanisms of the technology must be designed in a way that it corresponds with the expectations of the user.[1695] Margraf and Pfeiffer stress that this second element becomes more important the less technologies provide for a user-interface (such as currently happening in the Internet of Things). In conclusion, in order to safeguard that the internal mechanisms of a technology, which aims to implement privacy- and security-by design requirements, corresponds with the expectations of the user, the individual must be involved, as early as possible, in the technological development process.[1696] This technical approach corresponds to the considerations made previously with respect to the individual's decision-making process: If the individual concerned by the processing of personal data shall be able to effectively and efficiently manage the corresponding risks, this process must be designed in a way that the individual intuitively understands it.[1697]

Margraf and Pfeiffer propose to differentiate between the following three "trust-layers" in order to more specifically assess under which conditions the user accepts the privacy- and security-by-design measures, in

1694 See Margraf and Pfeiffer, User-centric development for the Internet of Things, pp. 246 and 247, referring to A. Whitten, J.D. Tygar: Why Johnny can't encrypt: A usability evaulation of PGP5.0. In 8th USENIX Security Symposium: Usenix, 169 to 184, 1999.

1695 See Margraf and Pfeiffer, ibid., p. 247, referring to J.H. Saltzer and M.D. Schroeder: The Protection of Information in Computer Systems. Proc. IEEE 63 (Sept. 1975), 1278 to 1308. Issue 9.

1696 See Margraf and Pfeiffer, User-centric development for the Internet of Things, p. 246.

1697 See above under point C. IV. 3. c) Conclusion: Specifying the decision-making process (Art. 24 and 25 GDPR).

other words, its usability:[1698] On the layer of "situational trust", the acceptance (that means, in this regard, usability) depends on the specific design of privacy- and security measures. However, the design is not the only aspect that should be taken into account. On the layer of "learned trust", the user has "learned" how certain mechanisms work or, on this basis, whether or not he or she can trust these pre-known mechanisms. This layer is particularly relevant with respect to the brand and reputation of data controllers. The user trusts in the data protection conformity of a certain data processing, pursuant to the cognitive association he or she has with the data controller's brand or reputation. In this regard, data protection certificates and seals are also particularly relevant because the user learns whether he or she can trust the data processing or not, if this occurs under a certain certificate or seal. Finally, the user's acceptance of data protection-by-design measures depends on "dispositional trust" that the user has, based on his or her personality. For example, if the user originates from a conservative milieu, it is likely that he or she trusts more in a seal given by a public authority than a private company. In contrast, if the user belongs to a modern-skeptical milieu, he or she trusts, likely, less in a seal given by public authorities than in the fact that the protection mechanisms are publically accessible so that scientific institutions can verify it.[1699]

3. Interim conclusion: Unfolding complexity

The preceding illustration of different methods for a risk assessment makes it clear that such an assessment can be rather complex. Basically, this complexity corresponds with the complexity of the technology and of the risks caused by the data processing, respectively. However, the preceding considerations have also shown that it is possible to adjust the assessment methods to the corresponding object of assessment. If the object of assessment is to research the risks caused by the processing of personal

1698 See Margraf and Pfeiffer, ibid., p. 247, referring to M. Friedewald, O. Raabe, P. Georgieff et al.: Ubiquitäres Computing: Das "Internet der Dinge" – Grundlagen, Anwendungen, Folgen, Berlin: Edition Sigma (Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag, 31), 2010.

1699 See Margraf and Pfeiffer, ibid., p. 248, referring to Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI): Milieu-Studie zu Vertrauen und Sicherheit im Internet, 2013.

data against abstract constitutional positions, such as democracy or solidarity, indeed, it will not only be necessary to conduct case studies. Instead, it will probably be necessary to work closely together with social science research disciplines, which may also conduct representative surveys at large, in order to understand a possible relation between the data material gathered from these case studies and/or surveys and the variety of theoretical concepts describing the functioning of democratic civil societies. Comparably, if the object of assessment is to capture and weigh potentially conflicting interests related to the data processing, the involvement of stakeholders concerned may be an appropriate means. Of course, each method has its difficulties. Roßnagel doubts, for example, that the theoretical concepts developed, so far, in social science research disciplines are already sufficiently advanced in order to explain, in a satisfying way the interrelationship between societal values, individuals, and technology, as a whole. However, in contrast, specific components of these theories may well suit a specific research approach.[1700] In turn, multi-stakeholder processes face the challenge, amongst others, of being rather complex and time consuming, which principally conflicts with lean and iterative development cycles for the technology in question.[1701]

In any case, in light of the variety of empirical (and interdisciplinary) research methodologies and methods, it is a primary task of legal researchers, who focus on the regulation of data-driven innovation, to find the research methodology and methods that are appropriate for answering their research questions.[1702] In light of the research questions posed in this thesis, the only method that was, so far, not yet examined in detail, appears to be particularly suitable: case studies. The main reason for this is not that case studies can simultaneously provide the basis for the two other means previously described (they may provide either a source of data for proving scientific evidence of theoretical concepts for the society at large, or as an illustration for potential points of interest conflicts between the stakeholders involved). Rather, in contrast to these other methods, case studies appear to be particularly suitable because of the following two reasons: First, they might particularly help understand *why* and *how* certain phenomena relate to each other; and second, they could be, in terms of co-

1700 See Roßnagel, ibid., pp. 182 to 185.
1701 Cf. Forum Privatheit, ibid., pp. 30 and 35.
1702 Cf. Hoffmann-Riem, Innovation Responsibility, p. 39; Roßnagel, ibid., pp. 287 and 288.

ordinated efforts, a less complex means. This could make case studies particularly suitable for de-folding very complex objects of assessments, such as in relation to non-linear innovation processes.[1703]

As illustrated before, the research approach of regulating innovation is, in light of its conceptual structure, a rather complex one. It does not only treat the question of protection against risks caused by data-driven innovation, but also, on the question of how such a regulation must be shaped in order to be open to or even enhance innovation. This approach hence adds another level to the question of how to protect individuals against the risks. The preceding analysis has carved out where the interplay between instruments regulating the processing of personal data becomes particularly clear: with respect to the question of how the individual's decision making process should be specified. On the one hand, thus, it is an open legal question of how this process must be designed, specifically, in order to provide the individual concerned by the data processing effective and efficient protection against the related risks.[1704] On the other hand, this room of flexibility provides data controllers the opportunity to find themselves the best solution and, therefore this kind of regulation is principally open toward innovation (at least, more open than classic if-then rules).[1705] Indeed, as illustrated in the preceding chapter "B. I. 2. Regulation of innovative entrepreneurship" of this thesis, this broader room of action decreases legal certainty, and this can in turn hinder entrepreneurial innovation processes. Thus, a promising solution could be to combine this principally broader room of action, which the principle of purpose limitation leaves, with further mechanisms increasing legal certainty in turn. Such a combination of regulation instruments may not only open to, but even, enhancing entrepreneurial innovation.[1706] For understanding this complex interplay, case studies can hence be a suitable means if the assumption turns

1703 Cf. Baxter and Jack, Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers, pp. 544 and 545; Eisenhardt and Graebner, Theory Building From Cases: Opportunities and Challenges, pp. 26 and 27.

1704 See above under point C. IV. 3. c) Conclusion: Specifying the decision-making process by means of regulated self-regulation.

1705 See above under point A. II. 2. The regulator's perspective, referring to Eifert, Regulation Strategies, cip. 59 and 60.

1706 See above under point B. I. 2. b) Principles between openness toward innovation and legal uncertainty.

out to be correct that they can explain, in particular, the *why* and *how* of phenomena.

II. Multiple-case-studies: Combining research on risks with research on innovation processes

A case study approach indeed faces certain challenges. Roßnagel stresses, for example, that the interdependencies of technology with its environment are often too complex so that it is hardly possible to describe it in a comprehensive and detailed manner, simultaneously. In his opinion case studies can therefore provide a basis for hypothetical risk scenarios. However, with particular respect to information and communication technologies, which are used in daily life, it is highly difficult to conduct those risk scenarios. He gives three reasons for this challenge: first, these technologies are usually used in very different contexts which makes it difficult to typify the risk-scenarios; second, the individual concerned, whose conduct is hardly predictable, constitutes an additional factor, influencing the technology assessment; and third, the interests of the stakeholders involved in the use of these technologies are, often, highly diverse.[1707] Nevertheless, Roßnagel stresses, in conclusion, that is not impossible to draw general conclusions from case studies. However, this may only be possible as the problem and the solution found are structurally generalizable and representative.[1708] This leads to the question of how case studies should be designed and conducted in order to provide such generalizable and representative results.

1. Reason for the case study approach

The economists Eisenhardt and Graebner particularly address this question – by refining it: How can theory, which is built on case studies, be generalized if the cases are not representative of all existing cases within this issue? They answer this question, hence, by refining the purpose of this empirical research method: The purpose of using a case study design "is to

1707 See Roßnagel, ibid., pp. 176 and 177.
1708 See Roßnagel, ibid., p. 188.

develop theory, not to test it".[1709] In light of this, case studies indeed "typically answer research questions that address 'how' and 'why'" of complex relationships amongst phenomena. In contrast, case studies are less suited "to address the questions 'how often,' and 'how many,' and questions about the relative empirical importance of constructs."[1710]

The philosophical approach that underlies a case study design may help explain this in a more illustrative way. In a nutshell, case studies are based on a constructivist paradigm, which understands reality as a "social construction". Thus, a case study can particularly suit this paradigm because it enables researchers to closely work together with the participants, whose actions shall be studied: Researchers can observe the participants in certain contexts in order to understand their view on reality and, though, the meaning of their actions.[1711] These considerations affirm the assumption made before that case studies can be a suitable means in order to understand, in particular, the complex functioning of the principle of purpose limitation as an instrument regulating innovation: On the one hand, case studies can assist, asking end-users of a data-driven technology, in answering the question of how data controllers should implement this principle by designing the individuals' decision-making process in a way that enables them to effectively and efficiently protect themselves against the data protection risks. On the other hand, case studies can help one to understand, by asking entrepreneurs who implement, as the controllers of the data processing, these requirements into their technologies, how they can use this room of action. In particular, under which conditions this room of action may not only be considered as giving more room for innovation but as even enhancing innovation?

1709 See Eisenhardt and Graebner, Theory Building From Cases: Opportunities and Challenges, p. 27.

1710 See Eisenhardt and Graebner, ibid., pp. 26 and 27.

1711 See Baxter and Jack, Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers, p. 545, with further references; cf. also Mayer-Schönberger, The Law as Stimulus: The Role of Law in Fostering Innovative Entrepreneurship, pp. 181 ff.

2. Generalizing the non-representative cases

These considerations confirm that case studies can be a suitable means for legal research on innovation. The question of how findings from such case studies can be generalized, remains still open. There are several techniques in order to make case study research more generalizable. Eisenhardt and Graebner recommend, in particular, to combine several cases to a single case study. In their opinion, "theory-building from multiple cases typically yields more robust, generalizable, and testable theory than single-case research."[1712] The reason is that only the relationships replicated across all or most cases has to be considered as relevant for generalization.[1713] With respect to the data gathered, through a multiple-case study design, the use of different data sources additionally increases the quality of the results because it reduces the bias of the information. For example, interviews with stakeholders concerned are a highly appreciated data source because they constitute an efficient way to receive "rich, empirical data".[1714] However, in order to avoid that the results of the analysis of interviews are limited to the subjective view of the interviewees, it is recommended to interview not only several individuals from different organizational levels and departments, in the same entity, but also from other relevant stakeholders outside the entity.[1715] Applying these recommendations to the research questions of this thesis, it is plausible to not only refer to the individuals concerned by data processing and people in the data controller's organization, but also to external observers. In particular, investors may provide, beside the individuals', an additional interesting data source because their powers often constitute a significant factor influencing how data controllers deal with data protection requirements. For example, if investors consider personal data processed by the data controller as an essential asset of their investment, they might require data controllers to comply with data protection law, just as they consider immaterial property rights as an essential economic value regarding their investment.[1716]

1712 See Eisenhardt and Graebner, ibid., p. 27.
1713 See Eisenhardt and Graebner, ibid., p. 30.
1714 See Eisenhardt and Graebner, ibid., p. 28; see also Baxter and Jack, ibid., p. 554.
1715 See Eisenhardt and Graebner, ibid., p. 28.
1716 See above under point B. I. 2. c) Interim conclusion with respect to the principle of purpose limitation.

3. Designing the case studies

Baxter and Jack finally provide guidance as to how case studies should be designed: In order to make sure that the cases selected can answer the research questions, as well as to determine the extent of generalization, it is necessary to determine a so-called unit of analysis, i.e. the "case". In doing so, Baxter and Jack recommend, for example, to clarify whether an individual (or entity) shall be analyzed, or whether a program, or process shall be analyzed.[1717] This question helps determine the unit of analysis for the empirical approach proposed in this thesis. The primary research question of this thesis concerns a "program", i.e. the functioning of the principle of purpose limitation established by the law. So far, this thesis has examined the following two questions, legally:

1. *What is the meaning and function of the principle of purpose limitation on the private sector, in light of the object and concept of protection of data protection law?*
2. *In order to find a balance between the societal need for data-driven innovation and protection against its risks, what regulation instruments should transpose the principle of purpose of limitation in the private sector?*

However, while the legal analysis could comprehensively answer the first of these research questions, the preceding analysis has demonstrated that the second research question cannot be answered by legal research alone. The remaining open questions essentially are, as summed up previously, how a data controller must specify the individual's decision-making process in order to effectively and efficiently protect the individual against related risks, and whether, or if so, under which conditions the specification of this process enhances its innovative activities. In order to answer these questions, it is now necessary to choose two sub-units of analysis: first, the process of the individual managing his or her risks in a certain context, and second, the innovation process of the data controller designing the individual's decision-making process. For the multiple-case study approach, these two phenomena are thus the two appropriate units of analysis.

After having determined the units of analysis, Baxter and Jack recommend to precisely define which aspects shall not be taken into account.

1717 See Baxter and Jack, ibid., p. 554.
See Eisenhardt and Graebner, ibid., pp. 545 and 546.

This helps avoid that the case finally becomes too broad. In order to avoid this problem, it is useful to provide for "boundaries", such as: by time and place; activity and context; and by definition.[1718] Boundaries are, apparently, helpful for the research questions of this thesis because these questions require, empirically, two units of analysis (even if they may partly overlap). Therefore, boundaries help "curb" the already broad approach resulting from such a doubled (or bridging) unit of analysis. Taking the examples given in the introduction of this doctoral thesis, it is possible to determine the cases pursuant to the following aspects: the time-frame in which the users use the products of the startups, as well as in which the startups process the data and conduct its innovative activities (e.g. developing and improving the product and/or business model); the place where the product is used (i.e. marketed) and where the startup is situated and operates; the specific activities of the users in their decision-making processes, and the startup's ongoing development process specifying the decision-making process of the individual (regarding the implementation of the principle of purpose limitation) and its efforts to turn this into a competitive advantage; the context in which the individual acts (which means, in particular, his or her substantial guarantees concerned by the processing), as well as the essential contextual parameters for the startup (e.g. the applicable law, customer segment, market, personal network); and, of course, the definitions of these terms (in particular, of the "principle of purpose limitation" as proposed in this thesis, of the term "business model", etc.).

Finally, the ultimate challenge of conducting a multiple-case study is to convincingly link the "rich" empirical data to distinct propositions that contribute to the research question. Eisenhardt and Graebner stress, in this regard: "If the researcher relates the narrative of each case, then the theory is lost and the text balloons. So the challenge in multiple-case research is to stay within spatial constraints while also conveying both the emergent theory that is the research objective and the rich empirical evidence that supports the theory."[1719] How the empirical findings may be linked to such distinct propositions shall be exemplified in the following chapter, by taking the examples of the startups mentioned in the introduction of this thesis.

1718 See Baxter and Jack, ibid., p. 554.
1719 See Eisenhardt and Graebner, ibid., p. 29.

III. Researching the effects of data protection instruments in regards to innovation processes

After having demonstrated that – and how – case studies can provide a suitable means in order to explain the complex interplay of regulation instruments and innovation, the approach shall now be illustrated taking the startups mentioned in the introduction as examples. As previously stressed, the legal analysis conducted in this thesis could comprehensively answer the first research question on the function of the principle of purpose limitation. In contrast, legal analysis alone cannot comprehensively answer the second research question of how the regulation instruments should be implemented on the private sector, in order to balance best the opposing fundamental rights. At least, it became clear that the instruments implemented for the decision-making process of the individual concerned constitute an essential object for such an interdisciplinary research approach: in first instance, it became clear that there are several remaining open questions regarding the effectiveness and efficiency of the protection instruments and that one has to put the end-user of these protection instruments into the center of the research process in order to find appropriate solutions.[1720] In second instance, one can now examine how this room of action can be used in order to turn this openness toward innovation into a situation that even enhances innovation.

1. Enabling innovation: Contexts, purposes, and specifying standards

The preceding chapter "B. I. 2. Regulation of innovative entrepreneurship" has carved out that this room of action is principally open toward innovation, but decreases legal certainty, which in turn principally hinders entrepreneurial innovation. The essential question therefore is how to combine the principle of purpose limitation that is basically open toward innovation with mechanisms that enhance legal certainty and, thus, innovation.[1721]

1720 See above under point D. I. 2. c) Specifying 'decision-making process' by user-centered development of privacy-by-design.

1721 See above under point B. I. 2. c) Interim conclusion with respect to the principle of purpose limitation.

a) Enabling data controllers to increase legal certainty

The entrepreneurial theories described before shed further light on this question.[1722] In the entrepreneurial environment, the law serves a condition for business opportunities.[1723] Correspondingly to the logics of causation and discovery, the regulatory "command-and-control" strategy provides the entrepreneur precise criteria of how to apply the law: Entrepreneurs must "discover" these criteria and build their products pursuant to them in a "causal-linear" process. However, in highly dynamic and non-linear environments, this regulation strategy risks turning into red tape with the result that legal certainty does not enhance but hamper innovation processes. In contrast, the legislator can also build on the creation and effectuation aspects of entrepreneurial behavior by establishing principles or broad legal terms and, correspondingly, through certain mechanisms that enable entrepreneurs to specify themselves how to apply the over-arching aim, and, thus, increase, by their own, legal certainty.[1724] Entrepreneurs have then to use the mechanisms that are "effectively" at their disposal and "create" their own criteria in order to make sure that the way they seek to reach the over-arching aim meets the legislator's expectations. Data controllers are hence able to increase themselves legal certainty, which increases their innovative capacities.

b) Enhancing competition on the "data protection" market

This leads, in addition, to a situation where the legislator helps itself create a market of innovation: By setting the over-arching aims, such as by the principle of purpose limitation, and leaving entrepreneurs sufficient room for its specific application, the regulator uses the creativity of private markets producing a variety of possible solutions.[1725] From a New Institutional Economics perspective, Wegner illustrates under which conditions a

1722 See above under point B. I. 1. Process of innovative entrepreneurship.
1723 Cf. above under points B. I. 1. a) Key Elements for the entrepreneurial process, and B. I. 1. d) Entrepreneurial Contexts: The Law as one influencing factor in innovation processes amongst others.
1724 See above under point A. II. 2. The regulator's perspective.
1725 See Wegner, Dynamic Markets and their Persistent Openness to Innovation, pp. 74 and 75.

regulator is able to enable such an innovative capacity.[1726] He argues that in light of the evolutionary nature of innovations, an economy's innovative capacity depends on the velocity of private entities to react to three constantly ongoing changes: First, to perceive current changes of scarce resources; second, to predict future changes; and third, on the basis of this information, to constantly re-allocate its resources. From this point of view, it is, a priori, impossible to centralize the knowledge necessary in order to determine future changes and, thus, the later profits of today's investments. The market as a whole thus cannot avoid that single investments fail; in contrast, the failure of investments is an essential pre-condition for the private entities' ability to learn.[1727] Wegner concludes from this that the legislator has only limited abilities to actively enable specific innovations: since it cannot centralize the necessary knowledge for such an active innovation politics, it can only guarantee the existence of competition in the market, and thus, that the market participants are able to make autonomous entrepreneurial decisions. Instead, if the legislator provides the company with a certain way of how they have to meet the regulatory aim, it minimizes their capacity to react to changes in their environment and, thus, their capacity of innovation.[1728] The regulatory strategy of "command-and-control" is therefore not able to maintain a market that constantly produces new ways of how the principle of purpose limitation is applied. This is another reason for why the legislator should be reluctant to define itself, too narrowly, the individual's decision-making process, beside the reason that such requirements can paternalize the individual concerned.[1729]

From this point of view, and given that no third parties' fundamental rights are threatened,[1730] it is the consumers' choice about the quality of products or services, i.e. the data protection level applied, which decides

1726 See Wegner, ibid., p. 73.
1727 See Wegner, ibid., pp. 74 and 75.
1728 See Wegner, ibid., pp. 76 to 80.
1729 Cf. the criticism of state-given decision-making processes ('choice architectures') at Neumann, Libertarian Paternalism – Theory and empiricism with respect to decision-making architectures designed by the State, pp. 41 to 55 and 97 to 100, as well as Sandfuchs, Privacy against one's will?, pp. 223 to 226, both referring to Thaler and Sunstein, Nudge – Improving Decisions About Health, Wealth, and Happiness.
1730 See above under point C. I. 1. b) bb) (2) A first review: decomposing the object and concept of protection.

on the success of innovations. This leads to a certain product and service variability of different qualities: If there is no common quality standard provided for by law, consumers who actually prefer a lower quality (for example, for a cheaper price) do not have to buy products or services of higher quality (and therefore for the likely higher price).[1731] Hence, the private entities create themselves, be it with the participation of the regulator (co-regulation) or without it (self-regulation), certain quality standards. These standards can then signal, for instance, in the form of certificates, the corresponding quality to the consumer.[1732] Indeed, the transaction costs that consumers have when they want to prove the quality in question can be prohibitively high. For instance, this might be the case if there is no common scale that helps compare the differences in quality. This case becomes particularly relevant with respect to the risks caused by the processing of personal data that most consumers are unable to foresee.[1733] Another case refers to the situation where the market for a certain product is so fragmented, that even if there was a common scale that principally makes a comparison of products possible, the consumer loses the overview.[1734]

However, addressing the first-mentioned problem, this thesis has elaborated on an objective legal scale that enables one to determine the specific risks caused by data processing and, as a consequence, to compare different levels of protection that data controllers may have implemented against such a risk. With respect to the second problem, consumer and/or data protection bodies may provide for a solution: If the market of different standards, such as in the form of certificates, is so fragmented that the consumers run the risk of loosing the overview, these bodies could evaluate the standards, compare and rank them, again, on the basis of the objective legal scale. This ranking signals the consumers, in an overview, which standards provide for which level of protection.

1731 See Wegner, ibid., pp. 84 and 85.

1732 See Wegner, ibid., pp. 85 and 86; Roßnagel, Data protection in computerized everyday life, p. 195.

1733 See above point A. I. 5 Interim conclusion: Uncertainty about the concept of protection and its legal effects.

1734 See Wegner, ibid., pp. 80 to 82.

c) Remaining questions in relation to the effects of legal standards

In conclusion, the legislator may thus not only provide for regulation instruments being open to innovation, such as principles or broad legal terms, but also enhance innovation through the establishment of mechanisms, such as standardization procedures as part of certificates. These mechanisms are able to enhance innovation on two levels: On the first level, standardization mechanisms enable entrepreneurs to create themselves legal certainty, which enhances their innovative capacities. On the second level, the legislator creates a market of innovation by creating and maintaining competition of different forms and levels of protection surrounding the principle of purpose limitation.

Indeed, there remain several questions about the effects of such standards.[1735] With respect to the legal effects, Eifert examines not only principles but also broad legal terms, where private standards play a role. This comparison provides greater assistance in order to obtain a better understanding about the possible variety of legal effects. Regarding broad legal terms, Eifert stresses, it usually belongs to legal courts to specify these terms. They fully control all interpretative executions of such terms by public agencies. However, in order to specify the terms, the Courts often refer to rules or standards set up by private entities, without acknowledging a direct legal effect of these rules or standards. Instead, they often serve as criteria for assessing the burden of proof or, at least, a reference for the judicial reflection.[1736] Such standards may play a role with respect to purposes specified within the law itself, such as marketing purposes in the ePrivacy Directive.[1737] In contrast, with respect to principles, private standards often serve to officially specify the principles. In these cases,

1735 See the definition of athe term "standard" by the International Organization for Standardization (ISO) and the International Electrotechnical Commission of Standardization (IEC) as a "document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context", retrieved on the 20th January 2017 from http://www.iso.org/sites/ConsumersStandards/1_standards.html.

1736 See Eifert, Regulation Strategies, cip. 61 to 63.

1737 See already under point C. I. 1. a) The interplay between European Convention for Human Rights, European Charter of Fundamental Rights and German Basic Rights, and see further examples above under point C. II. 2. a) cc) Further examples for different scales applied in order to specify the purpose.

there is often a functional separation of the entities dealing with private standards: one entity sets up private standards; the second entity seeks to apply the standards (e.g. entrepreneurs); and the third entity controls whether or not the second entity correctly applies this standard. Thus, the "control issue" is not carried by a public agency, but instead by private entities. Public agencies then control everything as a whole, whilst primarily focusing on the controlling entities.[1738] For example, the General Data Protection Regulation provides for several provisions regulating such standardization processes under its Article 40 to 42.

However, beside these general observations, there are many questions open to be answered by research. One question concerns the legitimacy of these private standards with respect to their legal effects. Since the legislator, who acts on the basis of democratic legitimacy, establishes broad objectives and, thus, is not able to guarantee, substantively, that private standards meet its objectives in detail anymore, it must guarantee the fulfillment of its objectives through procedural requirements. The General Data Protection Regulation addresses this problem, partly, by requiring the participation of the competent data protection authority in the standardization process, such as for codes of conducts and certificates under its Articles 40 to 42. In contrast, with respect to broad legal terms, such as purposes specified within the law itself, there are no such requirements. In any case, the question remains valid as to how standards can additionally be legitimized. One way for doing so, is by establishing so-called multi-stakeholder processes.[1739] As mentioned before, in these processes, the individuals concerned by the private standard are able to influence its establishing procedure. Of course, there are further remaining questions, such as how the multi-stake-holder process must be organized so that all interests of the individuals concerned by the standard are represented.[1740]

Another debated question is whether such standards may provide for the same level of protection as data protection law or must go beyond that

1738 See Eifert, ibid., cip. 91 ff.

1739 See above under point D. I. 2. b) Pre-structuring interests through multiple-stakeholder and expert participation.

1740 See Eifert, ibid., cip. 68, and Belli, A Heterostakeholder Cooperation for Sustainable Internet Policymaking.

legal level of protection.[1741] For example, Hornung and Hartl are of the opinion that standards can only fulfill their function as a market incentive if they provide for a higher level of protection than established by data protection law. They argue that the incentive consists in the marketing advantage that only exists, in their opinion, if the standard signaled to the consumers provides for a higher level of protection than what they could expect provided for by law. From this point of view, the "level of protection" provided for by law is a minimum level of protection.[1742] Irrespective of whether this general assumption is correct or not and without going into too much detail, the category of a fixed "level of protection" does not appear to fit the characteristics of a principle. As described before, a principle provides an objective, which, as its main characteristic, leaves room for the entities to find different ways of applying the principle. This allows, in essence, three different types of varieties: First, varieties of protection instruments applied with respect to different dangers, risks or threats for the individual concerned; second, given a certain danger, risk or threat, varieties of instruments ensuring the same level of protection (e.g. a private data broker acting on behalf of the individual concerned instead of a data protection authority); and third, given a certain danger, risk or threat, varieties of protection instruments leading to different levels of protection (e.g. opt-out instead of opt-in mechanisms). In light of this nature of legal principles, it does actually not make sense referring to a "minimum level of protection".

Finally, from an empirical perspective, there is not much research, if at all, on the practical effects of data protection standards on innovation processes. Blind examines, the effects of technical standards on innovation.[1743] Differentiating between several characteristics of standards (i.e. compatibility, minimum quality, variety reduction and information), he proposes the following overview on possible effects on innovation:

1741 See Hornung and Hartl, Data Protection through Market Incentives – in Europe, too?, ZD May 2014, who differentiate between audits referring to procedures ("dynamic character") and certificates referring to certain products or services ("static character").

1742 See Hornung and Hartl, ibid., pp. 220 and 221.

1743 See Blind, The Impact of Standardization and Standards on Innovation.

	Positive Effects on Innovation	Negative Effects on Innovation
Compatibility/Interoperability	Network externalities Avoiding lock-in in old technologies Increasing variety of system products Efficiency in supply chains	Monopoly power Lock-in in old technologies in case of strong network externalities
Minimum Quality/Safety	Avoiding adverse selection Creating trust Reducing transaction costs	Raising rival's costs
Variety Reduction	Economies of scale Critical mass in emerging technologies and industries	Reducing choice Market concentration Premature selection of technologies
Information	Providing codified knowledge	

Table: Types of Standards and their Effects on Innovation[1744]

How far these findings might be transferred to legal standards such as of data protection law is, indeed, another question. It appears to be plausible, at least, that legal standards, which typify the conditions under which a certain use of personal data meets the principle of purpose limitation, has similar impacts on innovation. For example, in the context of Smart Cities, a standard for the processing of personal data for the purpose of "creating social heat maps" might also have a positive impact on the network externalities of applications for traffic management. A plausible reason for this assumption could be that such a standard increased the legal certainty for startups (such as illustrated in the introduction, the social heat map application for traffic management) retrieving, transferring and exchanging corresponding data.

In any case, the interplay between legal certainty as an entrepreneurial incentive, compliance with the law (or its specific application) as a competitive advantage, and the functioning of co-regulation instruments on the private market is a rather complex issue. Therefore, the following examples, which were already mentioned in the introduction, shall help illustrate how the empirical case study approach, as proposed in this thesis, may answer some of these questions.

1744 Following Blind, ibid., p. 10, who refers to Swann, G. M. P. (2000), The Economics of Standardization: Final Report for Standards and Technical Regulations Directorate Department of Trade and Industry, Manchester Business School.

2. Demonstration on the basis of the examples provided for in the introduction

Applying the structure of this thesis, the following demonstration will first illustrate, for each single startup (i.e. "case"), how the specific application of the principle of purpose limitation can legally be analyzed. Subsequently, it will be demonstrated which remaining open questions could be answered by the empirical approach proposed above. With a particular view to the legal analysis, it shall be stressed that this analysis does not assess the compliance of the data processing with current data protection laws, except where it is explicitly stressed. Furthermore, the analysis does not go into much technical detail either. In particular, questions of data protection instruments against unspecific risks are not tackled in much detail. The focus of this analysis rather lies on exemplifying how the requirements to specify the purposes and to limit the later processing to the initial purposes may be met, in light of *specific* risks against the individual's fundamental rights.

a) Example of "personalized advertising"

In the first example, a startup sought, in the beginning, to analyze the usage behavior of the users of its mobile app in order to personalize image advertising. The users should be able to choose different background pictures for their mobile phones (so-called wall paper). If the users showed preferences for certain themes, the image advertising should match these themes, i.e. the corresponding user profiles. The startup wanted to sell these personalized image advertising spaces to companies from the advertising industry.[1745]

aa) Preliminary legal analysis

In light of the function of the principle of purpose limitation proposed in this thesis, the data processing can be analyzed pursuant to the specific risk that the purpose specified discovers.

1745 See above under point A. I. 4. b) aa) The unpredictable outcome of entrepreneurial processes.

(1) Initial product and business model: Internal freedom of development

The purpose described above discovers a risk for the users' guarantee of internal freedom of development. In particular, the processing of that data does not refer to the users' communications because the users' preferences are analyzed on the data collected irrespective of a communication process.[1746] The data only relates to their choice of background pictures on the phone. The data analysis does not refer, so far, to data related to criteria listed under Article 21 ECFR, nor does it reveal such information. Finally, the startup does not publish the collected data nor the profiles; in particular, it does not make the data available to their business partners from the advertising industry.

The appropriate instrument protecting the users against the risk for their internal freedom of development consists in providing for the information that the startup has about them. The information about their profiles, i.e. preferences shown for certain themes and, consequently, categories for the personalized image advertising, enables the users to know what the startup knows about them and, in particular, to protect themselves against the risk of being manipulated by the advertising.[1747] The startup could hence specify the purpose and make it explicit to the users as:

> "We collect and process data about your preferences that you show when using our app in order to, first, create a profile about your preferences and, second, personalize image advertising based on this profile. (We do not provide this data to our advertising partner from which we receive the image advertising.)[1748] In order to understand the profile that we create for your personalized advertising, you can always see here/below the current state of which categories we have created on which types of data collected in your case."

1746 Cf. BverfG, decision from the 22nd of August 2006, 2 BvR 1345/03 (IMSI Catcher), cip. 55 to 62.

1747 See above under point C. II. 3. b) cc) (3) Articles 7 and/or 8 ECFR: Information pursuant to insights into personality and possibilities of manipulation.

1748 From a substantial point of view, this sentence in brackets is not absolutely necessary because private data controllers do not have to exclude, explicitly and in advance, like state data controllers, further possible purposes, see above under point C. IV. 3. b) aa) (2) Extent of consent limiting the later use of data (instead of being illegal as a whole). However, private data controllers can, of course add this sentence in order to create more trust on behalf of the individual concerned. See also Article 13 sect. 1 lit. e and Article 14 sect. 1 lit. e GDPR.

This information should, as usual, be made available before the download of the app and be accessible when the app is installed on the phone. The blue highlighted term "here" or "below" leads the user, as promised, to the visualized information that is always kept up-to-date. On the basis of this information, the user is always able to understand why he or she receives these kind of advertising images and not others. This information is necessary but also sufficient in order to meet the users' guarantee of internal freedom of development and, in particular, in order to protect them against the risk of being manipulated by the advertising. Since these profiles reveal only a small aspect of the user's personality, and single out the individual only amongst the other users of the app, the processing does not directly affect the user's private life. Thus, there is no further need for a formalized process for the individual's prior and explicit consent. However, if the profiles become, in the course of time, so comprehensive and/or reveals particular aspects of the users' private life that this causes a higher risk for their substantial guarantee, the startup must send an explicit message to the users informing them about this higher risk and their possibility to opt-out, at least, from this higher risk. Indeed, when there is a higher risk for this substantial guarantee cannot be answered by legal research alone but should be determined together with other research disciplines.[1749]

(2) Change of product and business model: No substantive change of purpose

As illustrated in the introduction, the startup has changed, in the course of its development process, the functioning of its app, as well as its business model. The wall paper function of the app should now serve as an entry point for the user following the links to different media, such as music, newspaper articles, and still, image advertising. The startup sought to get a percentage from their media partners when its users purchase, having followed the link, a media product. This purpose did not reveal a new risk for another specific guarantee. In particular, the data processing did not concern the users' privacy of communications because the technological link

1749 See abve under point C. II. 3. b) cc) (3) Articles 7 and/or 8 ECFR: Information pursuant to insights into personality and possibilities of manipulation.

between the devices and the servers of the media partner still did not reveal a specific risk for the communication of their users.[1750] Another question is whether this new purpose constitutes a higher risk for the same substantial guarantee as already concerned before or not: the users' internal freedom of behavior. On the one hand, the new purpose covered, in addition to the personalized delivery of images, links to partners from the media industry. Insofar, one can say that the advertising is more intrusive because it makes it easier for the user to purchase a product advertised in the images. On the other hand, the user is able to recognize by him or herself the link to the offers made by the media partners. Either, he or she clicks on the link or not. Therefore, one could doubt whether this creates an additional risk of being manipulated or not. However, in terms of transparency and accountability, the startup should, at least, adapt the already existing protection instruments. This means, the startup should inform its users about this (only formal) new "purpose" and add this information to the already existent text described above. The copulation of this information makes it easier, if the data is used, later on, for further purposes, to trace the recent purpose back to all preceding purposes.

So long as the development process for the product and the business model does not reveal a risk for another guarantee than that of the internal freedom of development, the startup can proceed as described before.

bb) Open legal questions ('propositions')

Indeed, there remain several specific questions that cannot be answered by legal analysis alone. These specific questions can be used, turned around, as propositions for the case study. There are two overall questions of this study: First, how should the startup specify the purpose and, thus, the conditions for the data processing in order to enable the individual to effectively and efficiently manage the risks against his or her internal freedom of behavior? And second, under which conditions can the startup turn this, by means of standardization, into a competitive advantage?

1750 Cf. BVerfG, decision from the 22nd of August 2006, 2 BvR 1345/03 (IMSI Catcher), cip. 59 and 60.

(1) Standardization of "personalized marketing" purpose

The first question can be answered by assessing, together with the startup and its users, the following proposition: In order to enable the users to effectively and efficiently manage the risk caused by data processing for the purpose of "personalized marketing" against their internal freedom of behavior, the following aspects must be determined.

– At first, it must be clear which entity gets access to the information about the user. As described before, this is the startup itself. However, if further entities shall obtain access to the information, such as advertising or media partners, it must be clarified which entity is best suited for informing the user about which entity of them has which knowledge about the user.
– Correspondingly, it must be clarified about what the individual is informed of. If the user is able to know what others know about him or her, he or she has to know, at least, the profiling criteria under which personal data is categorized and which make him or her "unique", in relation to the other users in the profiling system. Furthermore, the user also needs information about where the data originates from and what type it is. The reason for this, is that it also determines the information about the individual. Finally, the user should know which entity specifically has that information.
– Furthermore, it must be clarified which protection instruments against unspecific risks the startup implements, as well as potential partners of the startup who receive the data or the information about the user. If the startup and, possibly, its partners, do not implement protection instruments against unspecific risks, the user cannot trust that the data and/or information is not misused, later on, because a third party gets access to that information without providing for the necessary protection instruments. Thus, the startup (or another entity that is better suited to inform the user) must inform the user also about these precautionary protection instruments. In this regard, also the information that no further entities than explicitly specified are able to access that information can enhance the user's trust that the information is not going to be misused.
– Finally, it must be assessed, how this information should be presented to the individual so that he or she is able, in terms of cognitive capacities available in the daily online life, to understand that information.

(2) Competitive advantage

Simultaneously and/or subsequently, the second question can be answered by assessing the following proposition: In order to enable the startup turning the standardization of this purpose into a competitive advantage, the advantages received for the implementation of the principle of purpose limitation and/or disadvantages avoided must outweigh, from the perspective of the startup, the efforts spent for it.

- With respect to the efforts, it is first necessary to decide whether the startup initiates itself a standardization process or whether it applies an existing standard. While the application of an existing standard enables the startup to signal a certain level of protection to its users, the initiation of the standardization process provides for an additional opportunity: The startup can influence this standard in favour of the specific risk and its specific needs, and potentially profit from a first mover effect. However, it is also more costly, if the startup standardizes itself the purpose.
- In any case, with respect to the advantages received and disadvantages avoided, it is possible to take, beside positive effects such as decreased transaction costs in light of higher legal certainty, the following network partners of the startup into account: Users, business partners, and investors.
  - Does the application of the standard help the startup to decrease the complexity of its entrepreneurial process, and if so to which extent? In particular, how decisive is legal certainty that they apply the law and are certainly not fined by a data protection authority?
  - With respect to users, it will be interesting to assess in which form the users of the app may favour the specific standard: Do they pay a higher price?; or do they use, more extensively, the app and therefore reveal more information about them?; do users prefer the startup's app to another product on the market that has no standardized level, or even a lower level of protection?
  - With respect to business partners, it will be interesting to see, for example, whether there are positive network externalities: Do business partners start exchanging personal data for the same standardized purpose for "personalized marketing"? Does this create a positive effect on the startup's data quality or increase the variety of products based on that data processing? Does it increase the startup's income, overall?

– Finally, do investors of the startup positively evaluate the economic value of the startup because it can certify the compliance of the data processing with data protection law?

Only if the startup comes to the conclusion that its advantages received or disadvantages avoided (e.g. fines because of data protection breach or legal uncertainty) outweighs the efforts spent for the standardization of that purpose or the application of an already existent corresponding standard, the startup is able to turn the legal requirements surrounding the principle of purpose limitation into a competitive advantage.

b) Example of "anonymized data for statistic/research purposes"

In the second example, a startup retrieved personal data from the social network Facebook via an API in order to create a social heat map. This heat map should predict how many people will be at a certain place and at a certain time. The startup sought to sell, pursuant to the first business idea, the social heat map to taxi drivers enabling them to plan their driving routes more efficiently. The data retrieved via the API related to geo-locations that Facebook users, who were organizing an event or attending such an event, have made public. This data was not anonymized when the startup gathered it, but the startup anonymized the data, immediately after having retrieved it, by deleting its references to the social profiles of the Facebook users.

aa) Preliminary legal analysis

In light of the function of the principle of purpose limitation proposed in this thesis, the data processing can be analyzed pursuant to the specific risk that the purpose specified discovers.

(1) Processing of public personal data: Self-determination in public

Since this data had been published before the startup retrieved it, the purpose of the data processing revealed a risk for the users' guarantee of self-determination in public. In light of this guarantee, it is important to note that the users published the data themselves. Facebook provides, at least

with respect to the function of organizing or attending an event, information for ensuring that the users are aware of the publication. Therefore, the first requirement provided for by this guarantee is met in that the first publication must be based on the users' consent (or, which is not relevant here, another legitimate basis provided for by law). Indeed, the startup's processing purpose did not concern the first publication of the personal data but its re-publication. In this regard, it is decisive that the startup had anonymized the data before it sold the social heat map to taxi drivers. So far, the purpose did not reveal a risk for the users whose data had been analyzed so that the startup did not have to implement further protection mechanisms. If the startup had not anonymized the data, it should have compared, taking the above-mentioned criteria into account, the original purpose of the first publication with the new purpose of the re-publication.[1751] However, since the startup anonymized the data, this mechanism did not play a role.

Nevertheless, the users' guarantee of self-determination in public also takes the possibility into account that personal data can be attributed, later on, by third parties, such as friends, family members, or colleagues. This leads to the moment where the taxi driver, once he or she has purchased the data, can attribute the data to the passengers.

(2) The taxi driver: Attributing anonymized data to passengers

The question of which form of anonymization excludes an application of data protection instruments provided for by Article 8 ECFR is particularly relevant with respect to the guarantee of self-determination in public. The reason is that the publication of data results in the situation that everybody else is principally able to relate the data back to the individual concerned. However, it depends on the anonymization technique which kind of additional information enables other individuals to de-anonymize or re-identify the data. As described above, the possibility to re-identify anonymized data can also be described in terms of risk. From a substantial perspective, the guarantee of self-determination in public hence determines which

1751 See above under point C. II. 3. b) bb) (3) Re-publication: Weighing 'interests' against 'old and new purposes'.

anonymization technique is necessary in order to avoid or, at least, reduce the risk for this guarantee.[1752]

In the case of the startup, there was a very low risk, at least a low risk being legally relevant for the individual's guarantee of self-determination in public. The reason is that the processing of the anonymized data leading to a possible re-attribution of that data to an individual concerned does not provide for an additional risk for his or her guarantee. A taxi driver picking up a passenger at an event because he or she was recommended to do so by the social heat map does not know more than if he or she had read the information published on Facebook by him or herself. The taxi driver simply gets notified that the individual concerned, i.e. the passenger, really was at the event. Indeed, the taxi driver would not be able to 'monitor' the published Facebook events by him or herself, in particular, not without such an algorithm. Thus, the data processing indeed enables the taxi driver to relate the data to a passenger, once he or she is at the location. However, this does not conflict with the passengers' right to self-determination in public. This might be the case if the processing leads to a serious interference of the individual's private life, for example, by connecting "a vast number of aspects" of his or her private life, which could not have been so easily connected otherwise, and by rendering this information ubiquitous.[1753] Another case can be that the processing reveals a single information (hence, no vast profile) but this information is particularly relevant for the personality of the individual concerned.[1754] However, the data processing by the startup, and the relation of that data to the passengers by taxi drivers did not constitute such a serious interference with the passengers' private lives. The purpose of the startup was to create a statistical social heat map, thus, the opposite of a personal profile (this was the reason for why the personal data could be anonymized). And the relation of that anonymized data "back" to the individual does not reveal a particularly relevant aspect of his or her private life. This is even then the case if the taxi driver picked up the passenger at a "delicate" location because the driver shows up at this location only because there is a statistic probability

1752 See above under point C. IV. 1. b) bb) (2) (b) Right of self-representation in the public.

1753 Cf. ECJ C-131/12 (Mr. González vs. Google Spain), cip. 80.

1754 Cf. Britz, Informational Self-Determination between Legal Doctrine and Constitutional Case Law, p. 572; BVerfG, 4th of April 2006, 1 BvR 518/02 (Dragnet Investigation), cip. 92 to 94.

that there will be enough people so that it is worth to adjust the driving route toward this location. This additional knowledge provided for by the social heat map is not particularly relevant for the passenger's personality.

In conclusion, so long as the purpose of the startup did not reveal another risk for the fundamental rights of the users of the social network, the startup did not have to apply any further protection instruments. In particular, it was not necessary to make the purpose explicit because there was no need for the users to adapt themselves to the informational measure or to contest it.[1755]

bb) Open legal questions ('propositions')

Here again, there remain, at least, a few specific questions that cannot be answered by legal analysis alone. The two overall questions of this case study are: First, how should the startup specify the purpose and, thus, the conditions for the data processing in order to reassure the individuals concerned, as well as the business customers of their application that the use of this application complies with data protection law? And second, under which conditions can the startup turn this, by means of standardization, into a competitive advantage?

(1) Standardization of "statistical" or "scientific" purposes

The first question could be answered by assessing, together with the startup, the following proposition: In order to increase legal certainty with respect to the data processing for "statistic" purposes, the following aspects must be determined.

– First of all, it must be clear to which extent it is possible, at all, to standardize the purpose of data processing for "statistics" or "scientific research". In particular, if the "anonymized" data is intended to be published, the risk that data is re-identified depends, first, in the context where the personal data originates; second, the technique used in order to anonymize the data; and third, the context in which the anonymized

1755 See above under point C. II. 3. b) dd) (3) (c) Protection instruments enabling the individual to adapt to or protect him or herself against the informational measure.

data is used. Therefore, a standard regarding "statistical" or "scientific" purposes has to be determined, at least, pursuant to these three categories. In the case of the startup, it appears hence to be plausible to limit the standard to personal data collected from social networks, and the publication of that data – anomyized, with a certain anonymization technique that must be specified – for the use in a Smart City, or more narrow, Smart City Traffic Management environment. In other cases, it might be necessary to specify the use of that data in more detail. For example, if the data shall be used for statistics in a military context, it is possible that this use conflicts, even if the data is collected in the (online) public and in an anonymized form, with the freedom of thought, conscience and religion under Article 10 ECFR of an individual. This can be the case if an individual is a deeply convinced pacifist, does not want that data originally related tom him or her is used in a military context, and did not know, when the personal data was collected, or could not avoid, that this data will once be used, in an anonymized form, for the statistics purposes in a military context.[1756] However, since this is not particularity the case, here, it does not have to be discussed which protection instruments might be necessary in order to protect Article 10 ECFR of an individual. So far, a limitation of the standard for "statistic" purposes to the criteria as proposed before seems to be sufficient.

– Indeed, the main challenge for this standard is to determine which anonymization technique reduces the risk of re-identification to a level where it is acceptable in light of the individuals' right to self-determination in public. One possible method is to assess, in the case study, by interviewing users of social networks, which risk scenario they are able to accept. These risk scenarios, and the results gathered from the inter-

1756 The reference to the individual's right to freedom of thought, consience, and religion can thus solve the question of which 'research project' is still covered by the 'research' purpose as discussed above under point C. III. 1. b) aa) (2) The more nuanced approach established by the Federal Data Protection Law, referring to Greve (Auernhammer), § 40 cip. 11 as well as Lindner, Data protection in the Federal State and the Länder, § 40 Rn. 23; in contrast, the Article 29 Data Protection Working Group apparently wants to exclude any impact on the individual, as described above under point C. III. 1. a) bb) (4) (a) Specification of the compatibility assessment (even ecluding positive effects), referring to Article 29 Data Protection Working Group, Opinion 03/0213 on purpose limitation, p. 28.

views, should additionally be re-assessed, with data protection authorities as well as experts from the field of anonymization, because of their higher expertise. The case study might lead to the result that further precautionary protection instruments are necessary in order to lower the risk further. For example, the startup might be obliged to give third parties access to that anonymized data only under the condition that they do not process the data in order to re-identify it.

– Finally, it must be determined whether, and if so, in which way the public must be informed about the data processing taking place under this specific standard. As illustrated previously, the data processing by the startup is not required to inform the individuals concerned, specifically. However, it may be necessary to inform the public in general, in order to re-assure users of social networks, once they get notified about the data processing, that pre-cautionary measures against the risk of a re-identification of the data are met. Only this information avoids that users suffer from the unspecific threat that the data might be misused, in the future. One solution could be that the social networks inform its users about the usage of that data under this specific standard. Another or additional way could be that the customers using that anonymized data inform, in a general manner, the public about it.

(2) Competitive advantage

Similar to the preceding case study, the second question can be answered by assessing the following proposition: In order to enable the startup turning the standardization of this purpose into a competitive advantage, the advantages received for the implementation of the principle of purpose limitation and/or disadvantages avoided must outweigh, from the startup's perspective, the efforts spent for it. In this regard, it is principally possible to apply the same propositions as already proposed in relation to the preceding case study. However, two particularities shall be highlighted. First, it might be particularly interesting to assess whether, and if so, to which extent the proposed standard will enhance a positive feedback from the business customers of the startup. This may be particularly interesting because passengers might find it "creepy" if they find out that their taxi driver plans his or her driving route on the basis of personal data (that they might have) published on Facebook, without further safeguards. Second, it will be interesting to assess in more detail whether the standard is "suffi-

ciently broad" enabling the startup to develop further business cases under the same standard (e.g. further categories of local public transport services, but also shops and restaurants). Such a flexibility is important because it would mean, otherwise, that the startup had again to standardize the purpose or to apply again an already existing standard. This would essentially increase the efforts spent.

In any case, if the startup comes to the conclusion that its advantages received or disadvantages avoided outweighs the efforts spent for the standardization of that purpose or the application of an already existing standard, it is able to turn the requirements surrounding the principle of purpose limitation into a competitive advantage, i.e. the principle has an innovation-enhancing effect.

c) Example of "scoring in the employment context"

Similar to the previous example, another startup gathered personal data that was already publically available. However, in this case, the individuals concerned have published the personal data not in a social but in professional networks. Furthermore, in contrast to the startup previously described, this startup did not anonymize the data. Rather, the startup processed that data, such as about steps of the users' carrier and their former places of residence, in order to create profiles about them. Based on mathematical-statistic methods, the profile of a user contained information about the estimated degree of professional experience in a certain area, the probability that he or she would change the current employer and/or his or her place of residence for another job. The startup sought to sell access to these profiles to human resource departments in order to assist companies to find new appropriate employees. Thus, this data was not anonymized and a negative impact was foreseeable because the information could appear so unattractive to an employer that it would not invite the individual concerned, albeit the individual might be interested in the job.

aa) Preliminary legal analysis

In light of the function of the principle of purpose limitation proposed in this thesis, the data processing can be analyzed pursuant to the specific risk that the purpose specified discovers.

(1) Re-publication of personal data: fair balance instead of a priority rule

This case is similar to the situation in the case of "*González vs. Google Spain*". As illustrated before, in this case, the European Court of Justice stated that a re-publication of personal data harms the individual's right to private life, if the re-publication is excessive in relation to the purpose of the first publication. In particular, the European Court set up, a priority rule in favor of the individual concerned affirming an individual's right to be delisted from search engine results, except if he or she plays an important role in public. Transferring this principle to the profiles created by the startup, the creation of the profiles and its usage by the startup's customers may be seen as excessive because of the negative foreseeable impact. The users of the social networks hence had, at least, a right to be de-listed from the startup's database because most of them do not play an important role in public.

In contrast, this doctoral thesis has criticized this approach as being oversimplified and referred, providing an example of a more differentiated approach, to criteria developed by the German Constitutional Court with respect to the German right to self-determination in public. The German Court at first differentiates, in this regard, as illustrated previously, between opinions and facts. In relation to the expression of opinions, the Court applies a priority rule favoring the freedom of expression if they contribute to the public debate. If the expression of an opinion primarily aims to defame an individual, his or her personality right prevails. If none of both rules apply, the German Court fairly weighs the conflicting fundamental rights.[1757] Applying this balancing exercise to the example of the startup, the discussion could develop as follows: First, it can be argued whether the result of the algorithm should be considered as a fact or an opinion.[1758] In order to answer this question, in general, the German Constitutional Court asks whether the statement can be subject to an obligation of proof: Opinions cannot be proven, but facts (also "internal" facts such as sentiments) can. In light of this criteria, it is clear that the personal data

1757 See above under point C. II. 3. b) bb) (3) (b) Excursus: Case law provided for by the German Constitutional Court, referring to Grimm, The Freedom of Speech in the judicature of the German Constitutional Court (Die Meinungsfreiheit in der Rechtsprechung des Bundesverfassungsgerichts), NJW 1995, pp. 1697.

1758 Cf. above under point C. IV. 1. a) aa) How data may be related to an individual.

used, such as the steps of carrier, places of residence and the number of former employees, are facts. However, the score based on these facts indicating, for example, the degree of expertise in a professional area is more arguable. On the one hand, the score is based on a certain mathematical-statistic method and can thus be understood and reproduced, objectively. However, this only proves whether the result is correct pursuant to the method. In contrast, the choice of the method used and, equally, the choice of the data analyzed in order to achieve a certain "forecast value" are valuing choices.[1759] This speaks in favor of considering these scores as opinions. Supposing this last consideration is correct, the subsequent question is whether the risk for the guarantee of self-determination arises from the valuing score or from the underlying facts. Since an employer looks, at first, at the score and, only, as a second step, at the underlying facts, it can be argued that the risk results from the expression of the opinion, i.e. the score, rather than from the underlying facts. The reason for this consideration is that the reduction of efforts that an employer has to spend analyzing the underlying data is, actually, the main value of the algorithm.

Therefore, it must be assessed whether a priority rule applies to this "opinion" or the opposing fundamental rights must fairly be weighed against each other. One question is, in this regard, whether this score primarily aims to defame the individual concerned. With respect to the start-up, its score is based on a mathematical-statistic method that has not the function to "defame" the individuals concerned. Therefore, the priority rule in favor of the individual does not apply. Hence, the other question is whether the opinion contributes to the public debate. If this is not the case, the priority rule in favor of the freedom of expression does not apply, either, and the conflicting fundamental rights have to be fairly balanced against each other. In this regard, further fundamental rights should also be taken into account. At this moment, it becomes apparent that the individual's freedom to find an occupation provides essential criteria for the balancing exercise. The reason is that even if the scores are principally available for everybody who pays the service of the startup, the information is particularly relevant for a certain social context, only: The employment- or work-related context covered by Article 15 ECFR. Thus, rather than the question of whether the scores contribute to the public debate *per se* or

1759 See Krasnow Waterman and Bruening: Big Data analytics: risks and responsibilities, IDPL 2014 (Vol. 4, no. 2), p. 92.

not, here, the specific freedom to find an occupation specifically determine the data protection instruments enabling the individual to influence his or her social representation in this work-related context. This leads us to the question of which instruments are necessary in order to find a fair balance between the opposing fundamental rights.

(2) Freedom to find an occupation: Participation instruments

Previously it was discussed in general, which instruments are appropriate for protecting individuals against the risks for their fundamental rights to freedom. In summary, if the controller or decision-maker reveals a risk, they must enable the individual concerned to adapt him or herself to the informational measure, contest and/or question it in public. These instruments shall now be illustrated with respect to the freedom to find an occupation under Article 15 ECFR: If a decision-maker in the human resource department informed the individual about the risk regarding his or her freedom to find an employment, it would be too late. The reason is that the employer has already received the information about the individual, and the individual could only react, afterwards. Therefore, the startup has to notify, before transferring the information to third parties, the individual about the transfer in order to enable the individual to avoid that the risk turns into harm. The startup could provide this notice, for example, via text messages within the professional networks. The startup could specify the purpose as:

> "Hi …, we would like to present you our new service for your profile. In order to help you find out which new carrier chances are out there, we process personal data that you have published under your profile about your current and former steps of carrier, places of work and employers. Based on this data we create a score about your professional experience, the likeliness of your interest for a new job offer, worldwide. If you would like to see your score, just click this link to our website where you can register with your LinkedIn and/or Xing account. If you would like to improve or adapt your score to your current situation, you can always correct the data you publish under your professional profile(s), and add new skills. So far, we do not take further score categories or categories of data into account. If you are interested in extending your profile and chances of your carrier, just contact us and we will do our best to extend your profile to further categories!"

Indeed, this text raises two essential questions. The first question refers to the extent of information that the individual needs to know about the func-

tioning of the score. In essence, the participation rights described with this information correspond to the right to correct wrong data and complete incomplete data. Furthermore, the user is also able to delete correct data, which he or she considers as having a negative impact on his or her score. The user is also able to see his or her score, so that he or she can evaluate which types of potential employers most probably prefer which skills or willingness to move and, thus, which data to add, change or delete. However, in order to effectively influence the score, the individual must be able to understand, at least, to a certain extent, the functioning of the score. Thus, it is decisive to assess which information the individual specifically needs. Indeed, this information right must be balanced against the opposing fundamental rights of the startup. The logic of the score might be protected by a patent, or as a business secret. In this balancing exercise, alternative protection instruments can also be taken into account. One alternative instrument could be, if the startup does not want to reveal the specific information about the functioning of the score that is needed by the individual, to provide information about the statistical reliability of the score. If the potential employer can see the degree of probability that the individual concerned really has the skills indicated in the score, this reduces the risk for the individual of not getting the employment offer even if he or she was an appropriate candidate.

Indeed, this alternative does not improve the position of the individual in his or her decision-making process with respect to these risks. This leads to the second question in relation to the text as shown above. Some readers may already have noted that this solution does not foresee a possibility for the user to forbid the creation of the score and the making available of this score to third parties. Hence, this solution does not implement an individual's right to be de-listed from the startup's database. Instead, the individual can only decide on whether he or she deletes data from his or her profile in the professional network, providing the basis for the scores, or not. This is a limited possibility for the individual to opt out-from the data processing. This opt-out procedure is limited because the individual can only opt-out from the startup's data processing if he or she deletes, in his or her profile within the professional network, all the data being relevant for the score. The following considerations shall exemplify how this question might be discussed, i.e. whether this opt-out procedure is sufficient in order to meet the individual's freedom to find an occupation or not.

First, the individual must have, as proposed previously, a right to opt-out from the data processing if this leads to a higher risk for the same substantial guarantee as already concerned before. In contrast, if the data processing leads to a risk against another substantial guarantee that was not specified before, the requirements are stricter, thus, an opt-in procedure may be necessary.[1760] With respect to the startup, its data processing leads to a higher risk for the same substantial guarantee "only". The purpose of the data collection and of its first publication within the professional network already referred to the professional context covered by Article 15 ECFR. Indeed, the original purpose did not make it explicit that there was a specific risk for this fundamental right. The users probably did not foresee, precisely, the risk of a third party creating scores with a potentially disadvantageous result, and which can be compared with scores of other users. However, the users knew, when publishing the personal data, that third parties will compare their profiles with others and, of course, will use this information as a basis for all kind of work-related decisions. Thus, even if this risk adds to the former situation because the score makes the comparison with a potentially negative result much easier than before, it is still the same guarantee of Article 15 ECFR that is at risk. Hence, an opt-out procedure might be sufficient.

However, this does not yet answer the question of whether it sufficiently meets the right to opt-out if the individual can delete, in the professional network, the data being relevant for the score. An answer to this question depends on the weighing of the individual's fundamental right to find an occupation under Article 15 against the startup's and employers' fundamental right to conduct a business under Article 16 ECFR. On the one hand, one might require that the individual is also able to object the creation of the score by the startup and its transfer to third parties, and is thus not obliged to "delete" his or her profile in the professional network. On the other hand, one might come to the conclusion that it is sufficient if the individuals concerned are able to: decide on whether to publish the data or not in the professional network; to delete some of this information or add further information; to see their score created by the startup; and evaluate the impact of this score for their future possibilities to exercise their fundamental right under Article 15 ECFR. Both options are plausible, and the

1760 See above under point C. IV. 3. b) aa) (3) Change of purpose: Opt-out procedures for higher and opt-in procedures for other risk.

balancing of the colliding fundamental rights may come to the result that both options are, from a fundamental right's perspective, possible.[1761] Indeed, the General Data Protection Regulation establishes an individual's right to object the data processing, pursuant to Article 21. If the startup bases its data processing on the general clause for its legitimate interests or the interests of the potential employers, the individual's right to object can be excluded only if it can demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject".

bb) Open legal questions ('propositions')

In light of the preliminary legal analysis, this case study should be designed, in particular, by focusing, on the one hand, on this decision-making process for the individual, and, on the other hand, on the impact on the startup's business model if this process is going to be changed.

(1) Standardization of "profiling potential employees"

The reason for this particular focus on the balance between the conflicting fundamental rights is that not only the risks for the individuals are particularly high, but also the impact of the startup's business model is significant if it was required to get the individuals more involved. So far, the value proposition of the application offered by the startup mainly refers to business customers. The possibility of the individuals concerned to delete personal data in their profiles within the professional network and to add further information is rather a side effect of this value proposition. In contrast, if the individuals have a right to opt-out from the data processing or the startup is even required to ask for the individuals' consent (in the meaning of opt-in), this turns the value proposition actually around. In this moment, the individual is able to keep its profile in the professional network as it is and, though, to freely decide on whether he or she wants the

1761 Cf. the variety of options exemplified by the German Constitutional Court, above under point C. I. 2. d) bb) In the private sector: The contract as an essential link for legal evaluation, referring to BVerfG, 23rd of October 2006, 1 BvR 2027/02 (Release of Confidentiality), cip. 59 and 60.

"service" or not. This leads to the result that the startup could be obliged, factually, to change its value proposition in a way which enables individuals to actively design their score, in order to keep these users in its "system".

Indeed, in particular, if individuals only have a right to opt-out, and are not asked for their consent, it may equally be possible that few individuals exercise their right to opt-out. This could lead to the situation that the few individuals, who opt-out, suffer harm from not being invited to job interviews only because the employer gets no score about them. This would hence be a situation where an opt-in procedure is required in order to 'nudge' individuals not to participate in the application, or even to forbid the individuals to consent. As stressed before, this can be justified if it is necessary to protect fundamental rights of third parties (i.e. the individuals who are not invited to job interviews only because there is no score about them). However, this is, so far, only a hypothesis, which can barely be assessed in case studies, today. And correspondingly, at least, a prohibition of the individuals' consent would not only harm, intensively, the individuals' but also the startup and employers' fundamental rights.

(2) Signaling legal certainty (to the "workers' council")

Therefore, it will be interesting to assess, in a case study, whether, and if so, which further incentives there may be for the startup to apply alternative protection instruments (e.g. information about the score's reliability). This might be the case if the startup's sales force fails, for example, when facing the workers' council of their customers, at least, in Germany. If the workers' council of the customer comes to the conclusion that the use of the application of the startup by the human resources department must be approved by the council, this might be a decisive incentive for the startup to re-assure the council that everything is compliant with the law. One important signal could be, in this regard, to standardize the purpose of that data processing, getting the data protection authority involved. And the data protection authority might approve the standard only if further protection instruments are set in place.

In conclusion, here again, there remain a few specific questions that cannot be answered by legal analysis alone. The two overall questions of this case study can be: First, how should the startup specify the purpose and, thus, the conditions for the data processing in order to re-assure its

business customers that the use of this application complies with data protection law? And second, under which conditions can the startup turn this, by means of standardization, into a competitive advantage? Only if the startup comes to the conclusion that its advantages received or disadvantages avoided outweighs the efforts spent for the standardization of that purpose or the application of an already existent corresponding standard, it is able to turn the legal requirements surrounding the principle of purpose limitation into a competitive advantage. Only in this case, the principle of purpose limitation has an innovation-enhancing effect.

5. Summary: Standardizing "purposes" of data processing

After having illustrated how these three cases could be studied, the question is which common patterns could arise in order to ascertain the general results?

At a first view, it appears to be difficult, indeed, to draw common patterns from these three cases. The reason for this first impression is that each case presented actually concerns another substantial guarantee: In the first case, the data processing leads to a risk against the internal freedom of behavior; in the second case, the anonymization technique used essentially determines the risk to the right to self-determination in public; and in the third case, the processing primarily causes a risk against the individuals' freedom to find an occupation. This diversity makes it difficult to draw generalizations, for instance, for the design of the individual's decision-making process. The situation would be different if all cases referred, instead, to the same substantial guarantee concerned by the data processing. For example, if in all cases the processing of personal data concerned a risk for the individual's internal freedom of behavior, but in different settings, it would be possible to generalize what information individuals need, in general, in order to distance themselves from own and other expectations.

However, second, there are certain commonalities. These commonalities refer altogether to the question of how purposes can be standardized, at all. Indeed, that the standardization of "purposes" stands in the center of this discussion is no coincidence. Previously, it was already stressed that standards appear to be an appropriate instrument increasing legal certainty for both the individuals concerned and the data controllers. The reason is that they signal, on the one hand, a certain level of protection to the indi-

vidual concerned and, on the other hand, reduce transaction costs of data controllers for complying with the law.[1762]

In any case, the preceding analysis made it clear that those standards do not refer to a certain product, procedure, or company.[1763] Instead, the standards discussed above refer to the purpose of the data processing. Referring to a purpose, instead of to a company, for instance, is possible, in particular, because the purpose is determined by the risk-based approach proposed in this thesis. In light of this approach, the primary question is not which company processes personal data or in which product or procedure the data is processed, but which substantial guarantee is at risk. This approach thus makes it possible, for example, to freely exchange personal data between different companies or products so long as the necessary protection instruments against this specific risk are met, thus, so long as this exchange does not cause a higher risk for the same substantial guarantee, or even a risk for another substantial guarantee.[1764] In conclusion, if personal data is processed under a standardized purpose, as proposed here, this means that both the individuals concerned and data controllers, which are part of this "purpose"-oriented system, are reassured that all data processing occurs under the same conditions.

The case studies also give the impression that it will be easier to standardize initial purposes than subsequent purposes, in particular, if the later data processing does not lead to a risk for another substantial guarantee that was not specified before. In all three cases illustrated before, the later data processing leads, "only," if at all, to a higher risk for the same substantial guarantee. The assessment of the risk against just one substantial guarantee is less complex than if several substantial guarantees have to be taken into account. This is in particular the case if a new risk for another

---

1762 See above under point D. III. 1. Enabling innovation: Contexts, purposes, and specifying standards"; in this regard, it shall be stressed, again, that the term "standard" does not necessarily mean an official standard provided for by an official standardization organisation such as the International Organization for Standardization (ISO); instead, a private standard can also be given the concrete form of a code of conduct or certificate or seal.

1763 See Hornung and Hartl, Data Protection through Market Incentives – in Europe, too?, ZD May 2014, who differentiate between audits referring to procedures ("dynamic character") and certificates referring to certain products or services ("static character").

1764 See above under point C. III. 2. c) Conclusion: Purpose limitation in decentralized networks.

substantial guarantee simultaneously increases the risk for a substantial guarantee that was already concerned before.[1765] However, it is not impossible to standardize, in addition, under which conditions personal data can be processed for another purpose causing a risk for another substantial guarantee that was not concerned before. These questions may become particularly relevant if private parties want access to certain personal data, for instance, in order to use it in the new context of "dispute resolution under civil law".

In any case, another common pattern will concern the question on the scope of risk that the standard covers: the standardization of purposes requires determining which processing purpose is covered and, thus, which risk. This definition influences two essential aspects of a standard: One the one hand, it determines the extent of trust that individuals and data controllers are allowed to have in the specific standard. If a certain standard guarantees that certain risks will not occur, individuals and data controllers can trust in this assurance. In contrast, if a certain standard does not tackle certain risks, individuals and controllers cannot trust that this risk will not occur because the standard does simply not cover this other risk. On the other hand, the definition of the standard determines the extent of efforts that must be spent in order to standardize the purpose and the corresponding conditions for the data processing. The broader the scope of risks is that a standard shall cover, the more complex the standardization process gets, and the more complex it is for companies to apply the standard, finally. Therefore, it will be necessary to assess the right balance between the broadness of risks covered and the complexity of the standardization process or the application of this standard. This balance will be decisive, at least, with respect to Articles 40 and 42 of the General Data Protection Regulation. As mentioned before, these provisions establish certain regulated self-regulation mechanisms enabling private associations of categories of data controllers and/or processors to draw up their own code of conduct or to provide for data protection certificates. Both provisions state that the "specific needs of micro, small and medium-sized enterprises shall be taken into account", when establishing such codes of conducts or certification procedures.[1766] One solution to reduce the com-

1765 Cf. above under point C. IV. 3. b) cc) (2) Examples: New risks not covered by consent (in light of the specified purpose), and C. IV. 3. b) cc) (3) Examples: New risks not covered by a former applicable provision.

1766 See Art. 40 sect. 1 and Art. 42 sect. 1 sent. 2 GDPR.

plexity of these procedures, avoiding that these smaller enterprises are overwhelmed, is to limit the scope of risks that the underlying standards cover.

Finally, there remains one last, but however very important, aspect to be clarified. It was shown that legal requirements, such as specified in standards, can enhance innovation, at least, so long as they do not turn "red tape". It was also illustrated that principles, like the principle of purpose limitation, are not "red tape" because they leave, in general, a certain room of action to the data controller, which is able to implement the principle pursuant to the particularities of a specific case. However, it may occur, indeed, that a change of purpose specifically endangers an individual's substantial guarantee so intensively that the principle of purpose limitation forbids the processing of data for this new purpose, overall. The data controller that has no overriding interest may perceive this restriction as a regulation turning "red tape" but this perception does not outweigh the individual's fundamental rights, of course. As stated in the introduction, the regulation of innovation does not require that each regulatory effect is open toward innovation or even enhances innovation. In contrast, the regulation of innovation makes primarily sure that the law does not *unnecessarily* hinder innovation, and in the second place, that it even enhances innovation.[1767]

1767 See above under point A. II. 1. Legal research about innovation, referring to Hoffmann-Riem, ibid., 260 and 261; cf. also Brownsword and Yeung, Regulating Technologies: Tools, Targets, and Thematics, p. 21.