E. Final conclusion: The principle of purpose limitation can not only be open towards but also enhancing innovation

This doctoral thesis has examined the principle of purpose limitation provided for by data protection law from the perspective of a "regulation of innovation". This approach examines both the risks caused by innovation and whether risk protection instruments are appropriate with respect to its effects on innovation processes. In light of this approach, this thesis has posed the question on, first, the function of the principle of purpose limitation in light of Article 8 ECFR, and second, which regulation instruments serve best, when implementing the principle of purpose limitation in the private sector, in order to balance the colliding fundamental rights of the data controller and the individual concerned. Pursuant to the previous analysis, the principle of purpose limitation is a regulation instrument that seeks, as a first step, to protect the individual's autonomy against the risks caused by the processing of data related to him or her with respect to his or her other fundamental rights. As a second step, it leaves sufficient room for data controllers to find the best solution for protection with respect to the particularities of the specific case. This scope of action enables, combined with co-regulation instruments, data controllers to turn the principle of purpose limitation into an innovation-enhancing mechanism.

The first component of the principle of purpose limitation requires the controller to specify the purpose of the data processing. This requirement is a precautionary protection instrument obliging the data controller to discover specific risks caused by its processing against the individual's (other) fundamental rights to privacy, freedom and non-discrimination. Whether the data controller must apply further protection instruments and, if so, which instruments precisely, and how, depend on the risk discovered by the specification of the purpose. How precisely the controller has to specify the purpose thus depends on the risk against the individual's other fundamental rights. For example, if the risk discovered by the purpose against a specific fundamental right to privacy or freedom requires the individual's consent, the purpose specified within the consent must precisely indicate the risk for this fundamental right. The data controller can reduce the risk against this right by implementing further protection instruments, such as further rights of information or participation of the individual in

the data processing. This may be necessary in order to find a legitimate balance between the risks against the individual's fundamental rights specifically concerned and the controller's fundamental rights and, thus, in order to legitimize the data processing, overall.

The second component of the principle of purpose limitation, i.e. the requirement to limit the data processing to the preceding purpose, aims to limit the risk caused by the later data processing to the risks previously discovered. Whether a risk caused by the later processing of personal data is compatible with the risk previously discovered or incompatible, depends, on the individual's fundamental rights to privacy, freedom and/or non-discrimination specifically concerned, on further protection instruments implemented by the data controller, and on the controller's opposing fundamental rights. For example, if the purpose pursued with the later processing discovers a higher risk for the same substantial guarantee (aka object of protection) of an individual's fundamental right to privacy, freedom and/or non-discrimination as previously concerned, the data controller may implement further protection instruments enabling the individual to manage the higher risk (e.g. informing the individual about this higher risk and giving him or her the possibility to opt-out from this risk). In contrast, if the new purpose discovers a risk for another substantial guarantee that was not concerned before, the requirements for such a change of purpose may be stricter. Particularly in this case, not only the new risk to this other substantial guarantee must be taken into account, but also whether the change of purpose additionally increases the risk for the guarantee initially concerned. The accumulation of risks might lead to the result that the change of purpose still is, in light of further protection instruments installed and the data controller's opposing fundamental rights, compatible with the preceding purpose, or is, definitely, incompatible.

This approach is a more refined approach than the current concepts of protection and therefore bears several advantages: First of all, referring the data protection instruments to risks against all the individual's fundamental rights avoids the situation that the scope of protection of the fundamental right to data protection becomes, in light of the increase of digitization in society, more and more, broad and vague. Since social interaction occurs, increasingly, on the basis of the processing of personal data, this approach makes it possible to differentiate, similar to the analogue world, protection pursuant to the different social contexts covered by the diversity of all fundamental rights. The approach thus provides an objective legal scale in order to reliably assess the risks caused by data processing. In do-

ing so, it helps to determine the scope of protection and also provides answers to further questions, such as which entity processing personal data must implement which kind of protection instruments. Such an objective legal scale is the first pre-condition for providing legal certainty.

The second advantage of this approach is that it provides a solution for the question of at which moment during the processing of data the regulation should apply: Is it necessary to regulate all potential risks the moment personal data is collected? Or is it sufficient to regulate the later use of that data? This question was already discussed in the 1970'ies and still is debated passionately.[1768] For example, Hoofnagle recently criticized, in a blog post titled "*The Potemkinism of Privacy Pragmatism*", the use-regulation approach because these "regulations offer no real protection, because businesses themselves get to choose what uses are appropriate" and, "understood in context, are part of what appears to be a general strategy to eliminate legal responsibility for data companies."[1769] These considerations are insofar correct as there is no objective legal scale determining when, in the life-cycle of a personal datum, a specific risk for certain fundamental rights occur and how these risks can be controlled before it irreversibly turns into a harm for the individual. In contrast, the previous analysis demonstrated that the fundamental rights of the individual concerned are typically concerned in different stages of the data processing: while the classic rights to privacy, such as at home or of communications, are typically concerned the moment that personal data is collected, a risk against the fundamental rights to freedom rather arises through the later use of data. This differentiated approach thus enables a regulation that is not only more effective, in favor of the individual concerned, but also more open toward data-driven innovation. The reason for this is that data controllers are hardly able to predict, when the data is first collected, all possible future purposes of data processing because the outcome of innovation processes is hardly predictable. However, in light of the approach proposed in this thesis, the principle of purpose limitation does not require data controllers to predict all possible purposes, in advance, because the

1768 See above under point B. II. Risk terminology oscillating between 'prevention' and 'precaution', referring, amongst others, to Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, p. 1221.

1769 See Hoofnagle, The Potemkinism of Privacy Pragmatism: Civil liberties are too important to be left to the technologists.

principle does not exclusively refer, with respect to the evaluation of the risks, to the moment of collection, but to all later moments, equally.

This leads to the third advantage because the proposed approach is not only open toward innovation but is also able to enhance innovation. On the basis of an objective legal scale, data controllers are able to specify the principle of purpose limitation with respect to the particularities of its specific data processing. Indeed, this does not disburden them from the so far required case-by-case assessment. However, by means of regulated self-regulation mechanisms data controllers can set up private standards for specific cases that are, however, generalizable. How this can be done in a reliable, scientific way was demonstrated in the last chapter of this thesis. In particular, applying a multiple case-study approach makes it possible to standardize certain purposes of data processing in a way that guarantees that the individual's decision-making process is so designed that individuals can effectively and efficiently manage the risks caused by the data processing (i.e. determined by the corresponding purposes). Such standards, be it in the form of a certificate, a code of conduct or binding corporate rules, specify the conditions of the data processing and can thus signal to the individual concerned, as well as business customers of the data controller, the level of data protection. Data controllers can hence create themselves legal certainty and use this as a competitive advantage on the market.

Finally, such standards simultaneously provide the basis for two additional advantages. First, they provide the basis for further privacy-enhancing technologies. If machines shall, one day, manage the risks on behalf of the individual concerned, the purpose of the data processing and, thus, all further requirements must be formalized, at least, to a certain extent, in order to enable machines to communicate the requirements to each other. In particular, formalizing purposes makes it possible that a third party (potentially, a machine), which receives personal data from another party (or machine), can obtain all purposes previously specified in an automated way. Indeed, this does not automatically safeguard that the principle of purpose limitation is actually met. However, the documentation of the preceding purpose is the necessary pre-condition for the purpose compatibility assessment; and in a world of ubiquitous computing, it is hardly imaginable how all the corresponding purposes are documented and exchanged, other-

wise.[1770] To which extent this requires manufacturers to implement the technological parameter into the soft- and hardware that they produce, is another question.[1771] In any case, standardizing purposes will be, in light of the decisive role that the requirement of purpose specification plays in data protection laws, an essential pre-condition for the success of data protection-by-design.

Last but not least, pursuant to Article 46 sect. 2 of the General Data Protection Regulation, such standards can safeguard the transfer of personal data to third countries. In particular, with respect to the USA (but also, soon, to the UK), such standards may particularly help increase legal certainty for the exchange of personal data. Mainly focusing on Nissenbaum's context-based approach, this thesis has shown that the general discussions about the object and concept of the privacy and/or data protection approaches are, actually, not so distinct as it seems. The outcomes of both approaches often are, in practice, rather similar.[1772] In light of the similarities, standards may therefore help, indeed, further bridge the transatlantic divide, be it under a data protection or privacy regime.[1773]

1770 See Roßnagel, Data protection in computerized everyday life, pp. 162/163 and 165.

1771 See Roßnagel, Data protection in computerized everyday life, p. 192; Schulz and Dankert, ‚Governance by Things' as a challenge to regulation by law.

1772 See Maxwell, Principles-based regulation of personal data: the case of ‚fair processing', p. 213.

1773 Cf. Kift, Bridging the transatlantic divide.