CHAPTER 4

Regulation as a Facilitator of Startup Innovation: The Purpose Limitation Principle and Data Privacy

Max von Grafenstein

Abstract Personal data are permitted to be used only for the purpose for which they were originally gathered. This is the basis of the 'purpose limitation principle', which, as one of the key pillars of German data protection legislation, is often hotly debated. The use of this principle is a challenge, not only for startups but also for individuals affected by the processing of their personal data. Where startups often do not know how data may finally be used, and therefore find it difficult to specify precisely or broadly enough the purposes to which a user's data might be put, affected individuals often find themselves in a labyrinth of possible purposes to which their data might be put followed by an endless series of data protection conditions. Users often emerge none the wiser regarding the possible purposes to which their data might be put. Therefore this chapter discusses how the purpose limitation principle might best be applied. The proposal given here allows a non-restrictive, indeed innovation-friendly, application of the principle.

M. von Grafenstein (✉)
Alexander von Humboldt Institute for Internet and Society, Berlin, Germany

© The Author(s) 2018

N. Richter et al. (eds.), *Entrepreneurial Innovation and Leadership*,
https://doi.org/10.1007/978-3-319-71737-1_4

Keywords Purpose limitation • Legal certainty • Data protection model • Standards • Certificates • Purpose standardisation

The Purpose Limitation Principle: Between Innovation and Legal Certainty

Data protection legislation in general and the purpose limitation principle in particular exist to protect those affected from threats which they cannot anticipate. Such threats can emanate from use of their data by internet start-ups, whose business models are often based upon the processing of personal data. For example, users of social media usually assume that the startup which operates the network uses the data collected to drive its services and the personalisation of advertising. However, they might be surprised to discover that this, or another startup, uses the data to calculate their creditworthiness—and shares this result with lending institutions, who subsequently approve or disapprove credit or the interest rate to be applied. The purpose limitation principle is intended to protect people from these kinds of unforeseen applications of personal data—and herein lies the problem. Startups have a limited ability to anticipate future uses of data. The strict application of the principle limits the degree to which new content, products, services and business models can be developed. This is particularly the case for Internet-based innovations: development processes are not linear and strategically planned: they are dynamic, emergent and often spontaneous. The results of innovation processes are typically open ended.

This chapter uses results from the Alexander von Humboldt Institute Research Group 'Startup Clinics' (Alexander von Humboldt Institute for Internet and Society, n.d.), which conducted a Law Clinic for startups over a four-year period (see also Chaps. 2 and 3). Four other Clinics were also offered to startups to assist them in their startup endeavours. The Law Clinic analysed the business models of over 100 client startups from a legal perspective, including the effect of the purpose limitation principle on their innovation processes. In the course of this research, it became clear that discussions surrounding data privacy and the purpose limitation principle are characterised by a significant lack of precision. Three key points were consistently overlooked during discussions about the principle,

hindering progress towards resolving the tensions between innovation and legal certainty.

One significant building block required to resolve the tension is the creation of data protection legal standards, which are allowed for in the European General Data Protection Regulation (GDPR) in the form of certificates and behavioural guidelines. Using such standards, those organisations responsible for data protection legislation can work with data protection agencies to clarify the legal requirements. This leads to best-of-breed solutions for particular industries (such as insurance) or certain products and service categories (such as e-health apps). Lawmakers are simply not in a position to acquire and apply sector or product specific regulations with the speed required by the highly dynamic and innovative Internet economy.

Therefore, instead of regulating every conceivable area in detail, lawmakers can express their decisions regarding values and acceptability in the form of legal concepts and principles, whose formulation allows scope for self-regulation. In this case, data processing organisations can work with data protection agencies to generate the required industry, product and service knowledge. This process will generally be far quicker and more efficient than the formal law-making procedures. This will require collaborative preparatory work before the actual creation of standards. This aims to create objective measures which can be used to formulate and concretise the purpose limitation principle.

Intended Purpose and the Purpose Agreement in Data Processing

It is noticeable that in debates around data protection and the purpose limitation principle the individual components of the principle are not clearly stated. The first component is the requirement to explicitly state the purpose. This provides the foundation for the second component, that the data may only be used for the purpose that was originally stated and agreed to. Furthermore, the various constitutional protection concepts which determine the functions of these two components are not drawn out. The European Charter of Fundamental Rights contains an independent protection concept which differs from the German right to information self-determination. It is often overlooked that Article 8 Paragraph 2 of the Charter does not state any purpose limitation or earmarking, but

only states that a purpose should be specified. The determination of the data's purpose by the data processing organisation is necessary in order to answer the question whether further legal demands should be made of the data processing. One such additional demand can be that of the purpose appropriation. But the constitution does not demand this, at least not according to the Article 8 of the Charter; and the GDPR does not articulate any strict purpose appropriation. The provision only really demands that the processing of personal data should not be inconsistent with the original purpose. Whether this is so can only be resolved by examining each specific case. The concept of protection in Articles 7 and 8 of the Charter has a significant influence on the application of any such case-by-case examination. Clearly, a precise definition of the concept of 'protection' can provide important criteria to startups and help them to reliably assess the application of the data purpose limitation principle for their specific case.

Missing Measures for Purpose Limitation

This leads to the second significant, and often neglected, aspect of purpose limitation. Before the question of consistency between purpose and actual data processing becomes relevant, the question of the precision of the formulation of the purposes of the data collection must be addressed. The more broadly the purposes have been formulated, the less need there will be for these to be changed to allow for subsequent unanticipated data processing. If, for example, the original purpose of the data is that it be used for marketing purposes, then there is no need to reconsider subsequent processing which is directed towards marketing—irrespective of the specific type or aspect of marketing. The GDPR does not address the specification of the purpose and leaves this up to each individual case examination. Unfortunately, this provision provides no criteria for specifying the purpose of the data collection. In the same way, as argued previously, a clear constitutional data protection concept could provide important guidance. The absence of such criteria leads to a high level of legal uncertainty for (internet) startups, who are responsible for data protection and also for those whose data are to be protected. As long as it is not clarified, how precisely these data are to be used, neither the data processing organisation nor the affected users can establish whether the use is permitted or not. Article 29 on Data Protection takes a position on the use of the principle of purpose limitation, but on closer inspection it provides hardly any

reliable criteria. The main criterion contained here is purpose consistency (not purpose limitation): the context of the data processing, the kind of data involved, the gap between the new and the old purpose, the possible consequences for the affected party and the protection measures are to be considered. But the Article does not describe how a context is to be defined, how the 'kind of data' is to be classified, how the gap between purposes is to be measured, how to determine the consequences or how protection measures are to be selected or activated.

The Right to Personal Privacy, Liberty and Equality as Standards for Data Protection Mechanisms

In order to address the legal uncertainty, a first step might be to apply all fundamental rights of the Charter, rather than try to limit the analysis to a general basic right to information privacy as described in Articles 8 and 7. The progressive digitalisation of society threatens to render other fundamental rights less important than those about data protection described in these two Articles. This was clearly visible in the so-called Google Judgement. Google was forced to delete the link between the name of a person and the occurrence of their name in an (otherwise legitimate) article about them. The German Constitutional Court has until now examined such questions from the perspective of public self-presentation and freedom of opinion. In contrast, the European Court has focused on data privacy and protection laws, in most cases giving these priority over competing basic rights. In such cases, the court refers to the purpose of the initial publication of an article and the subsequent purpose of the linking of terms via a search engine—without any further specification of what these activities entail.

Such an unclear conceptualisation of this state of affairs has substantial consequences. In the future, the more social behaviour and opinions are developed on the basis of information generated through automation, the more legal conflicts will be carried out under the banner of 'data protection rights' rather than on the basis of other rights. As such, it will become increasingly difficult to tease apart and assess how these other rights are being affected. As long as debate is only carried out in the terms of data protection, the question will immediately be referred back to itself. In contrast, the totality of fundamental rights—the right to personal privacy, liberty and equality—could provide a more refined set of measures to

Fig. 4.1 The data protection model

determine the legal position of data processing and the precision required of the data purposes.

If one uses the various guarantees of fundamental rights as presented in Fig. 4.1, it becomes possible to measure the danger of manipulation of individuals through targeted marketing, including its effect on their fundamental right to individual autonomy: one can assess the threat of monitoring and invasive data collection of employees using the concept of professional freedom and use scoring processes against the set of fundamental rights. The purpose limitation principle achieves a new level of functionality by expanding its interpretation to the danger posed by transgression of this principle to various basic rights. The purpose can be articulated broadly or narrowly depending upon the threat posed to those fundament rights.

Standardisation of Data Use Purposes: A Prerequisite for Designing Privacy by Design

The question of the precision of the stated purposes to which data can be put, as well as the reconciliation of purposes to actual use, can be resolved by the use of objective measures. How can this be put into practice? Even if objective measures were to exist, in order to do this reliably every data processing step would have to be assessed. The startup engaged in data processing must ask, for every data processing step, whether this is a new

purpose and is therefore not allowable. Have we established this clearly and is it consistent with the original purpose? This examination involves significant effort and expense—resources which are usually not available to startups.

The next step in resolving this issue would be the standardisation of typical and routine data processing steps. Data processing organisations should work together with data protection authorities in Standards Committees, which can react quickly and flexibly to the new challenges by formalising and publishing different types of purposes for different contexts. Both users of Internet services and data processing companies could rely on the legitimacy of these data purpose standards. This would encourage innovation and speed without endangering legal certainty.

This idea became more and more convincing during the daily practice of the Startup Law Clinic (see also Chap. 3). In sessions with startups, the various purposes of data processing were discussed. Only in a very few cases was a clear and final legal opinion possible, regarding the formulation of the purpose of the startup's data collection. Even when a startup used external lawyers to suggest formulations and approved these formulations for use, the users were rarely helped, and complained of lack of clarity and confusion. This impression has been confirmed in a number of studies. For example, the Ofcom paper' 'Personal Data and Privacy' looked specifically at the role of the informed consent. They found '*that the consumer seldom reads the conditions of use and if they do, they generally have difficulties in understanding them. It is difficult or even impossible for any consumer to understand the consequences relating to the use of their personal data*' (Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, n.d.). With this in mind, a standardisation of purposes for data use may provide an important building block for a practicable and meaningful consent.

Advantages of Standards: The Case of Certificates

It is of course easy to cast doubt on the extent to which such purpose limitation standards can be implemented and how enthusiastically they will be taken up. It is important to emphasise, though, that purpose limitation standards would not be universal: not all instances of data processing would need to adopt standardised purposes, only those that wish to.

There are many advantages to the standards approach. Most importantly, such purpose limitation standards would serve to minimise the legal

uncertainty which arises in the current case-by-case examination. Startups would only have to verify that the data processing they envisage falls under a certain standard: this standard would be communicated to the affected party or user. Under these circumstances, the startup can use the data according to this standardised purpose in all subsequent data processing phases. The use of standardised purposes would make it clear to the affected parties how their data might be used. The same effect would apply to changes in purpose. In fact, the GDPR anticipates such privileged use, at least for standards which take the form of certificates. At the very least, the data protection requirements contained in a certificate give a level of confidence that subsequent data processing applied to a person's data will comply with the law and regulations.

The use of certificates can also ensure that data transfer to third parties or other countries is still supported by a legitimated legal framework. This is of great interest for data exchange with the United States and the United Kingdom. In the USA, the future of the so-called 'Privacy Shield' is uncertain, owing to recent legal and political developments. The exit of the UK from the European Union will reduce the country's status to that of a third party. Data transfer to such countries could be legitimated through the use of certificates, as these can be anchored in appropriate control and sanction mechanisms. Organisations outside the European Union can gain access to personal data from the inner European market if they adhere to the control and sanction mechanisms of standards, for example in the form of certificates.

Open Questions for Purpose Standardisation

In the final analysis, standards have the advantage of being more efficient and streamlined than lawmaking. Standards bodies can react more quickly to technological, economic and social developments; and, as is appropriate, the GDPR allows that the certification processes consider the needs of small and medium-sized enterprises. In contrast to this, cumbersome lawmaking processes often produce laws which are outdated by the time they are implemented. Legal standards for data use purposes can provide a balance between innovation and legal certainty—and therefore create an important foundation for a well-functioning data ecosystem. Of course many questions remain open. The most important of these is whether the GDPR allows the standardisation of data processing purposes. A strong argument in favour of this is that the appropriate prescriptions relate to

specific data processing tasks, and these tasks cannot even be considered for initiation by an organisation without a statement of purpose. The standardisation of the data processing steps would contain the processing purpose. A further open question is how detailed and precise such standardisation will need to be in order to achieve the required level of legitimacy and trust—especially in the minds of those affected. Finally, and in reality, it is not clear whether powerful Internet companies will accept such standards or prefer individual case-by-case examination. Nevertheless, as long as standards do not exclude other means of assessment, it is unlikely that they will do any damage.

This chapter provides suggestions for the application of the purpose limitation principle to the practice of data processing organisations as well as the everyday use of systems by consumers. Internet-based startups, which in the course of rapid and radical innovation move in a domain of great uncertainty, may profit the most from suggestions such as these (see also Chap. 1). More work is required to add detail and depth to these ideas, and many questions remain open. The level of detail which is required to describe a particular purpose, or whether a new purpose is consistent with the original one, can only be resolved by consulting with those affected. Only when users understand and trust the data use conditions, and are confident that subsequent misuse of data is excluded, will they use the services and products from which data is to be gathered. The same is true of organisations that purchase data-oriented applications from startups for their own use. The organisations are more likely to purchase them when they can be assured that they are not transgressing data protection laws. Standards, for example in the form of certificates, may provide a useful means of sending clear signals to users and organisations about the consistency of data use with relevant data protection laws.

References

Alexander von Humboldt Institute for Internet and Society. (n.d.). *Innovation und Entrepreneurship*. Retrieved from: https://www.hiig.de/en/project/innovation-and-entrepreneurship/

Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste. (n.d.). *Personal data and privacy*. Retrieved from: http://www.wik.org/index.php?id=687