Chapter 7
Redesigning Data Protection

Frederick Richter

Introduction

When it comes to redesigning a consolidated system of judicial perceptions and well-known rules like those of continental data protection, first of all, it would be necessary to justify and to provide reasons for this intention. And as any modification of a law brings more than negligible expenditures with it, a need for justification and reasons applies to larger reforms as well as to minor changes.

So, do recent rules for protecting people's private information and personal rights need to go through a complete transformation, or is it only a matter of fine adjustment? Are there any severe shortcomings? Below, some seemingly small points will be lifted out of the broader discussion. These points need some more light shed on them in order to make them more visible in recent debates regarding the use of personal data. Quite often in these debates, well-known assumptions and theorems are not scrutinized sufficiently. For a German Lawyer, it's even harder to do so, because our common attitude is to deem our law as nearly perfect and worth being exported and spread globally.

This is exactly what we did in the area of personal rights. We codified the world's first data protection law in 1970 in the German federal state of Hesse. With our Federal Data Protection Act of 1977, we gave strong guidance for the EU's 1995 Data Protection Directive. Finally, in 2012, it was mainly German experts in the European Commission and Parliament who wrote the draft of the General Data Protection Regulation—very likely always keeping in mind the German law on data protection, which had been time-tested for nearly four decades.

F. Richter (✉)
German Foundation for Data Protection, Leipzig, Germany
e-mail: richter@stiftungdatenschutz.org

D. Feldner (ed.), *Redesigning Organizations*,
https://doi.org/10.1007/978-3-030-27957-8_7

The Conventional Idea

Such knowledgeable tradition could be seen as a perfect starting point to build upon when it comes to creating future-proof rules on handling personal data. But in some respect, there is a danger of seeing the well-known way of regulation as the only way. Sometimes it seems that German and European lawmakers have become blind to some already notorious shortcomings of continental data protection law.

In the 1970s, when the seeds of recent European data protection laws were sewn in Germany, it was conceived as a right of defense against actions of the state—a state that was increasingly able to store and process large and structured amounts of data. One such state action in the following decade was the planned census, which was feared to incommensurately investigate German citizens.

The German idea for how to comprehensively protect human beings from dangers that might occur to their privacy and personal rights was nearly a perfect one. We simply put the right to decide what other people—and most of all, organizations like public authorities and private companies—know about the affected person into the hands of that very person. The inventor of this idea called it "informational self-determination" (Steinmüller 1971). In 1983, this legal concept figure was elevated to the rank of a fundamental right (Bundesverfassungsgericht 1983). Since then, the German state has been called upon to ensure that a citizen is always able to know *who* knows *what* about him, *when* and *on what occasions*.

Some believe that, even then, this objective was merely idealistic. In any case, in order to ensure such comprehensive knowledge of the individual's data use in the long term, it would be necessary to limit the handling of data to a level that is still manageable, or at least graspable, for the individual person. Technology continued to develop over the decades, while the core principle of data protection law stayed the same—regardless of the amount of data that the individual should be able to decide about for himself. The amount of data has increased massively. And it keeps rising, every month. It continues to rise with each new method of recording, with every single sensor being added the myriads of devices connected in the "Internet of Things", as well as with each reduction in costs for storage space.

Although the wording "informational self-determination" has not made it into either the German or the European data protection law, its basic idea of perfect personal protection by total data control still prevails: A natural person shall have the widest possible control over the data concerning her or him at any time. Any use of such personal data is initially forbidden by data protection law until either the person concerned permits the use or another legal permission takes effect.

There Is No Such Thing as an Informed Consent

If a person has legalized the processing of their data by consent, then it should only be natural that this consent is given on the basis of knowledge and understanding.

If the person does not know and understand what shall happen to her or his data, then free self-determination can no longer be seriously assumed.

If the means and ways of using, evaluating and linking personal data are becoming increasingly complex, then the law must respond to this. It must ensure that the information base on which consumers make decisions regarding the handling of their data remains broad. With further technological development, the information base must become all the better in order to continue ensuring self-determination. What does the recent law have to offer in this context? It simply tries to cope with the growing challenge of informing people as much as possible by offering specifications for the linguistic design of privacy policies and for the design of information pages for digital services. This answer is not sufficient.

The General Data Protection Regulation, adopted in 2016, defines consent as a "freely given, specific, informed and unambiguous indication of the data subject's wishes" in a statement or a clear affirmative action (Article 4 (11) GDPR). If declarations of consent are pre-formulated by a company, they should use "clear and plain language" (Recital 42 GDPR). At first glance, these requirements seem very plausible and, moreover, easy to implement for the data-using economy. But what does compliance with the law mean in concrete terms at this point? Using the much sought-after "simple language", pre-formulated explanations of consent will become even longer than before, because frankly it takes many more words to explain a legally and technically difficult issue in simple terms. To the same extent that a privacy policy grows, the willingness of users to read it drops. It is therefore possible that comprehensibility increases, while the level of true information on the user's side decreases. It is not enough for the legislator to rely on the existence of an ideal user—someone with a lot of time in today's fast moving daily routines and with the disposition to read lengthy terms and conditions of digital services.

A Solution on One Page?

There are a few ways to address the problem. One approach is to try to display the most important parts of the content of a privacy policy on only one page, so that as few users as possible are discouraged from reading simply by the sheer amount of information to be read. These one-pagers, promoted by the German Ministry of Justice and for Consumer Protection, are merely an additional source of information; they are not meant to replace any formal data protection declaration, because they summarize and inevitably simplify in a way (BMJV 2016). It is assumed that users will not read the full declaration after having read the one-pager. But also the proponents of the one pager concept would have to rely on users to read the page. And this is the crucial and sore point: in the vast majority of cases no data protection declaration gets read at all. With regard to the effectiveness of this promising approach , it has been scientifically

found that, among consumers, the feeling of being informed does not increase with the summary being on one page (ConPolicy 2018). Further efforts will therefore be needed to approach a truly informed consent.

Transparency and Control

Knowledge and awareness are therefore indispensable for the data subject—and citizens cannot acquire sovereignty with regard to their own data without an overview and certain control. How many people know to whom and where and when they have given which consent for the use of their data? How many of these permissions to use personal information were not revoked, even though they were no longer in the interest of the data subject—just because the person no longer knew that they had given this consent? They need overviews and controls—via some digital dashboard or other technical solutions. Perhaps it is not primarily a task of data protection law to foster such innovative tools. But lawmakers and politicians are called upon to be more open minded toward news ways of dealing with the widespread problem of the uninformed customer.

The German Foundation for Data Protection took this unsatisfactory finding—too little openness concerning new solutions among the data privacy community—as an occasion for a project dealing with potential technology-supported improvements to the situation of consent. Some questions formed the starting point for the investigations: To what extent could technical consent assistants and consent platforms ensure the strengthening of rights to information, the automation of the consent process, the clarity and intelligibility of consent and the transparency of data processing purposes? What solutions—both internationally and in Germany—already exist, and where is further research necessary and worth promoting? We compared a number of very different practical experiments and theoretical approaches from the realm of the "Personal Information Management Systems—PIMS" (Horn et al. 2017).

The evaluation of technical possibilities and solutions in the field of PIMS shows that many approaches could create the preconditions for the legal processing of the relevant data and enable access rights or rights to restrict the processing, erasure or digital oblivion of data without requiring repeated direct user interaction. In this way, they would simplify the consent process. The approaches were analyzed from the point of view of how to create transparency through automated creation of an overview of the access rights of various applications; how to let the user decide individually in advance who should receive what data and for what purpose; how to enable users to take control by providing an overview of usage and how—in terms of self-protection of their data—to motivate consumers to control their data by exercising their rights to information. The examined projects showed significant differences, both in terms of their technical approach and economic implementation. They also differ in terms of how extensive the effect of the application is. For example, a specific approach may only have one focus (e.g., pure user education), or it can combine several different purposes.

How About a Consent Agent?

A particularly outstanding innovation would, of course, be a real consent agent, a tool that implements and executes the user's privacy preferences according to his specifications. In the ideal, such a "privacy-bot in the service of man" would not only be able to give consent in the sense of the data subject, but would also contain a database of consent declarations issued. This functionality would bring users much closer to a state of having a good overview and control in the data area.

But of course, such tools would need to fully comply with the GDPR, which is the supreme point of orientation in the area of data protection and the respective legislation for at least the next 5 to 10 years. And as the GDPR includes specific stipulations for consent, there are certain challenges for that new idea of user control. For example, to meet the conditions of GDPR Article 4, Paragraph 11, a clear confirmative action is needed from the consent assistant. Similar to any data controller under the rules of the GDPR, a privacy agent/data protection assistant would also need to explain the circumstances of any planned or programmed consent in easily accessible and understandable language to its user, including the type of data affected, purposes, recipients or categories of recipients. Developers of privacy assistance tools will also have to face the challenge that blanket consents are not valid. So it would not be possible for a user to generally instruct their privacy app to provide consent in a multitude of cases, for instance "for all cases where location data is requested by a Belgian app" or "for all apps requesting car-related location data" or other groupings like that.

For the functioning of a privacy assistant, it would be required that data protection declarations and privacy policies become machine-readable. The tools would need to assess what the vendor of any "opposite side" offers concerning the use of personal data from the user. But also, any automated translation of data protection instructions for a consent statement (for example, in the form of a list whose empty fields must be activated by the user) must be subject to verification in each individual case. This requirement might decrease the effective usability and convenience of consent agents. Difficulties might, for instance, arise if the data protection information references contract-related purposes, or if a consent statement is generated from this on an automated basis according to user preferences. However, no consent is required for contractual purposes, only transparent information. If the consent assistant is used in future to assist in the conclusion of contracts, then civil law and data protection law will have to be separated. Under civil law, consensual statements of intent are required for the formation of a contract, and as *essentialia negotii* of a purchase contract, this also includes the definition of the subject and the contracting parties. From a data protection perspective, data may be processed without consent if it is necessary for contractual purposes. Nevertheless, transparent information about the data processing (such as processing for contract-related purposes) must be provided. In designing the consent assistant, care must be taken to ensure that this separation is clear to the user.

Additionally, from a data protection perspective, consent always includes a right to revocation. With regard to the exercise of the right to revocation, any new system should offer users a self-management function, so that users can change, correct and delete their consent at any time. Thus, the requirements for a revocation from GDPR Article 7, Paragraph 3 can be met. Problems that could arise in connection with the new right to data portability (Article 20 DGPR) would then be bypassed. The necessary accuracy of the data may be ensured by the system if the consent assistant is able to prevent those types of data access in which the recipient, purpose and scope of the specific personal data do not match. The potential recipients have access to the records of users only on the condition that the right combination of legitimate recipients and processing purposes are present. In cases of deviations, the consent assistant must also be able, in dynamic form, to request and obtain the consent of the user.

As part of the design of the consent assistant, the coupling prohibition and free consent by the relevant parties must be observed to a special degree. All the circumstances must be taken into account, as well as whether the person can actually see in full the marketing and/or scoring purposes for which the personal data is used. This self-determination can be difficult to determine in certain individual cases. But the more purposes are interrelated, or the more data recipients are involved, the more likely the confusion for the person concerned. When using a consent assistant, the impression must also not be created that, as a result, the data processing is complete—especially if, for example, additional processing is planned for a legitimate reason. The legal requirements of such 'dynamic consent' must be examined separately.

The consent assistant should be able to automatically ensure that consent is not granted for an indefinite period, but that data access will automatically be prevented—either when the purpose of use no longer applies, or if after an appropriate time the user is asked if he/she wants to maintain his/her consent. In this case, the restrictions on data storage (GDPR Article 5, Paragraph 1e) and data minimization are fulfilled (GDPR Article 5, Paragraph 1c), since the person concerned decides what data is processed and that access is subject to the declaration of consent together with the category of recipients. The person responsible for the data processing must provide the consent on an informed basis. He must provide the information prior to collection of the data and must be able to show proof of consent. To support the transparent design of the choices (purpose, recipient, data) and in the interest of an informed and unequivocal expression of will, a consent assistant could—perhaps even should—apply visual elements (GDPR Recital 58). For complex data processing with different purposes or recipients, the representation could well be anything but transparent, even if a consent assistant were used. Regarding this, it could be examined to what extent the so-called one-pager mentioned above would be useful as a transparent summary of the consent given.

Overall, it should be noted that the legal requirements of informed consent and consent platforms would be difficult to establish without additional insights into economic behavior. Providing transparent information is a necessary—but not a sufficient—condition for an accurate assessment of data protection risks. In this respect, the emotions and cognitive abilities of the user are just as important, if not

more important. In other words: the legal framework for informed consent can only be assessed and structured appropriately if the actual willingness of users to actively deal with the protection of their privacy is taken into account. Finally, it must be noted that it is always crucial to ensure the future achievement of the General Data Protection Regulation's aim of putting in place a uniform and high level of protection for natural persons, by applying an equivalent level of protection for the rights and freedoms of natural persons with regard to the processing of their personal data in all member states. In this context, it is particularly useful to consider uniform codes of conduct or guidelines. In practical application, a consent assistant with transparent design possibilities can contribute to the level of protection. Users have more control over their options, since data can be collected directly from them with their active participation and can be limited in time. However, technical developments must constantly be critically examined against a background of automated decisions, the possibilities of profiling and a change of purpose.

Towards a Layered Approach

In order to approach real informational self-determination, a high level of information is indispensable. Certainly, this will not be attainable using just one of the possible methods. Rather, the solution can be sought in combining them. In order to meet the different requirements for the provision of information for the intended data processing, a multi-layer model should be used. The aim is to have the best-informed consumers. The multiple layers are in the best interest of consumer policy—and they should also be in the best interest of the economy, because they are proof for companies that they have sufficiently fulfilled their information obligations under data protection law.

The bottom layer in the proposed model consists of a machine-readable data protection declaration. To this end, it is necessary for the legislator to lay down guidelines for the structure of such declarations in order to ensure uniformity. This also facilitates the use of privacy bots that can capture and evaluate the content of a privacy statement. As a second layer, the first visible-to-the-user layer builds up on the machine-readable base layer. It is the full declaration on compliance with data protection law, written by lawyers and read only by other lawyers (usually those of the competitors). This layer corresponds to the "long" version of the data protection information that we know today and which, on its own, brings no innovation whatsoever. But this well-known—and well-hated—standard element is supplemented by the third and fourth layers. The third consists of the above mentioned one-pager. Reading it requires less effort and perseverance than the "full" explanation. But the effort is already considerably more manageable if a single page is to be read instead of ten or more pages. If the content of a page is already too much for the reader, the reader can go back—or better: step up—to the fourth level. It is the crowning conclusion of the information pyramid, so to speak. It consists of symbols or little pictures like those used in the license system of Creative Commons. Even current law

would not need to be re-designed. The GDPR already mentions such "standardized icons" in Article 12, Paragraph 7. The icons should give "a meaningful overview of the intended processing.in an easily visible, intelligible and clearly legible manner". But since the final version of the adopted new European data protection law does not contain concrete examples of icons, work remains to be done, supported by politics and research. Initial proposals have been made in the past and new ones are being added (Specht 2018). However, we still have important tasks ahead of us, especially in the area of design and implementation.

References

BMJV. (2016). Federal Ministry of Justice and Consumer Protection—"One-Pager"—Muster für transparente Datenschutzhinweise. www.bmjv.de/DE/Themen/FokusThemen/OnePager/OnePager_node.html. Accessed April 10, 2018.

Bundesverfassungsgericht. (1983). Federal Constitutional Court, Judgment of the Second Senate of 15 Dec 1983 –1 BvR 209/83–, para 172.

ConPolicy. (2018). *Better informed? Results from behavioral science on the effectiveness of the privacy-one-pager approach and further solutions for data protection.* www.conpolicy.de/en/news-detail/better-informed-results-from-behavioral-science-on-the-effectiveness-of-the-privacy-one-pager-appro. Accessed April 12, 2018.

Horn, N., Riechert. A., & Müller, C. (2017). *New ways of providing consent in data protection—technical, legal and economic challenges*. https://stiftungdatenschutz.org/english/project-consent-pims. Accessed April 10, 2018.

Specht. (2018). Informationsvermittlung durch standardisierte Bildsymbole—Ein Weg aus dem Privacy Paradox? In *Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung 2018.*

Steinmüller. (1971). *Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern*. German Bundestag printed paper VI/3826, pp. 5–224 www.dipbt.bundestag.de/doc/btd/06/038/0603826.pdf. Accessed April 10, 2018.

Frederick Richter, LL.M. is director of the German Foundation for Data Protection (Stiftung Datenschutz). After studying law at the University of Hamburg, Richter completed a master's degree in information law at the Universities of Vienna and Hanover. After completing his legal clerkship in Berlin, he was admitted to the bar in 2005 and worked as a research assistant to a member of the German Bundestag. From 2008 to 2010, he was a consultant and data protection officer of the Federation of German Industries (BDI). From 2010 to 2013 he was a consultant in the German Bundestag on copyright and network policy. In 2013, he was appointed founding director of the Stiftung Datenschutz. Frederick is a member of the IAPP and sits on the advisory boards of the projects AUDITOR for data protection certification and ABiDa—Assessing Big Data at the University of Münster. He is a member of the Data Protection and Ethics Panel of the AXA Group and permanent author of the journal Privacy in Germany (PinG).