forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVACY AND SELF-DETERMINED LIFE IN THE DIGITAL WORLD

Policy Paper

EVALUATION OF THE GENERAL DATA PROTECTION REGULATION

IMPRING

Authors:
Alexander Roßnagel[1], Christian Geminn[1], Maxi Nebel[1], Tamer Bile[1], Dara Hallinan[2]

(1) University of Kassel, project group Constitutionally Compatible Technology Design (provet) at the Research Center for Information System Design (ITeG)
(2) FIZ Karlsruhe – Leibniz Institute for Information Infrastructure

Contact:
Michael Friedewald

Telephone +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Series:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1st Edition, February 2020

Introduction

After more than four years of negotiations, the General Data Protection Regulation (GDPR) entered into force on 24 May 2016 and has been applicable since 25 May 2018. According to Art. 97(1) GDPR, the European Commission is obliged to submit and publish a written report on the evaluation and review of the Regulation to the European Parliament and the Council by 25 May 2020 and every four years thereafter. According to Art. 97(4) GDPR, the Commission must take into account the positions and findings of the European Parliament, the Council and other relevant bodies and sources. According to Art. 97(5) GDPR, the Commission must, if necessary, submit appropriate proposals to amend the Regulation and, in particular, take into account "developments in information technology and … the state of progress in the information society".

This policy paper takes the upcoming evaluation as an opportunity to point out possible improvements to the Regulation and to make concrete suggestions. The paper emphasises that the Regulation has brought about many positive innovations for data subjects: for example, the extension of the scope of European data protection law through the principles of market place and observation, data protection by design and by default, strengthening the rights of data subjects, the right to data portability and the extended possibilities for sanctions. Nevertheless, it should not be overlooked that the Regulation – due to shortcomings in its conception and wording – has not only created new deficits but has also failed to eliminate existing deficits. Above all, due to its high degree of abstraction, it is not suitable for addressing the specific challenges of modern and future information technologies. The deficits mentioned are of both operational and conceptual nature and are addressed accordingly below.

This policy paper aims to contribute to the discussion on how to improve the General Data Protection Regulation. It is limited to selected aspects that should be given priority in the upcoming evaluation.

Operational shortcomings

Significant improvements in the protection of data subjects are possible by addressing six main problem areas, which need to be revised and clarified. These are presented below and specific suggestions for improvement are made.

The relationship between consent and the other grounds for lawful processing

The relationship between consent and the other grounds for lawful processing is unclear due to the Regulation's wording. In this regard, by using the term "at least", Art. 6(1)(1) GDPR creates the impression that several legitimate grounds for processing can be applied side by side. The wording in Art. 17(1)(b) GDPR could also be understood in the same way with regard to consent under Art. 6(1)(a) GDPR since, according to this provision, a revocation of consent only gives rise to a claim to data deletion if there is "no other legal basis for the processing". According to this interpretation, the controller could, for example, invoke a balancing of interests under Art. 6(1)(1)(f) GDPR if the data subject has revoked his or her consent to data processing and thus "retreat" from one ground to another.

On the one hand, the General Data Protection Regulation combines different information obligations with different types of authorisation. The controller must specifically refer to and inform a data subject as to the legitimate ground relied on. If the controller relies on a balancing of interests, he or she must inform the data subject prior to data processing about the underlying legitimate interests and their predominance, as well as about the possibility of objection under Art. 21 GDPR. If the controller wishes to rely on the data subject's consent, he or she must inform the data subject, before consent is given, about the possibility, and legal consequences, of revoking consent – namely that further data processing is not permitted after a revocation. However, if the controller were then to rely on a balance of interests, he or she could take the view that the revocation would be formally ineffective and refuse to interpret it as an objection under Art. 21 GDPR. This could also lead to the data controller providing the data subject with contradictory information, as part of the duty to inform the data subject before the start of data processing about all possible permissible facts. In addition, the data controller would have the option of initially keeping several possible permissions open and only deciding on a particular permission later on – for example, if the permission is revoked or contradicted.

This also affects the right to data portability under Art. 20 GDPR. Data portability was celebrated as an innovation of the Regulation, but only applies to personal data processed based on consent pursuant to Art. 6(1)(1)(a) or Art. 9(2)(a) GDPR or on the basis of a contract pursuant to Art. 6(1)(1)(b) GDPR. The wording of the provision is clear and conclusive here, so that, for example, personal data processed based on legitimate interests pursuant to Art. 6(1)(1)(f) GDPR are not covered from the outset. From the data subject's perspective, whether this right is held or not may be of importance to the data subject when giving consent. However, if controllers can subsequently switch to legitimating data processing on a balancing of interests, they deprive the data subject of his or her right to data portability.

By subsequently changing the ground for processing, the controller would be violating the principle of fairness under Art. 5(1)(a) GDPR. The principle covers the manner in which rights are exercised between the controller and the data subject. This must be "fair" and must not unduly disadvantage any of the parties involved. Fair data pro-

cessing must therefore at least include that the data subject can be certain that exercising his or her rights will also have the expected legal consequences, i.e. that consent will establish the right to data portability and that the revocation of consent will actually render future data processing inadmissible. Otherwise, the controller could act under the pretext that the data subject has decision-making power, only to bypass this power later.

In view of these contradictions, the Regulation should make it clear that the controller cannot invoke another ground for processing in addition to consent. If a controller requests consent from the data subject, then the controller must also comply with the *rules* on consent. In particular, the controller must then accept a revocation of consent and may not, despite revocation, continue data processing with reference to another ground for processing; in addition, the controller must allow the data subject to receive and transmit his or her personal data.

Avoidance of personal data

The principle of data avoidance is one of the general data protection principles. Before the reform of the data protection law, it was legally anchored in German data protection law. It is an effective way of guaranteeing the rights of the data subject and should therefore be implemented in European law as well. The principle demanded that the avoidance of personal data be taken into account when determining the purpose, i.e. that the controller is obliged to select a specific purpose in such a way that as little personal data as possible is required for processing. However, the General Data Protection Regulation regulates the principle of data minimisation in Art. 5(1)(c) GDPR. At first glance, this appears to be synonymous, but on closer inspection, this is not the case. Data minimisation stipulates that data may only be processed to the extent that it is necessary as a means to achieve the purpose of the processing in question. However, dissimilar to the aim of data avoidance, the controller is free to choose the (legitimate) processing purpose and to design these in such a way that all the personal data they want to collect are also deemed necessary. This chosen purpose is limited by the General Data Protection Regulation only by the generally formulated data protection principle of fair processing pursuant to Art. 5(1)(a) GDPR. Since the extent to which this principle influences the choice of purpose by the controller remains open, the current wording could mean that the controller can process disproportionately more personal data as long as they adjust the purpose accordingly. Whether the requirement of data avoidance can be read into recital 78 sentence 3 GDPR – which clarifies that Art. 25 GDPR requires that the processing of personal data be minimised – remains an open question. This is the case as, in case of doubt, this collides with the codified principle of data minimisation in Art. 5(1)(c) GDPR. For this reason, it would be desirable, for the effective protection of fundamental rights, if data avoidance were to be embedded in law within the Regulation. The best way to do this would be by clarifying the data protection principles, specifically in Art. 5(1)(c) GDPR, in which case sanctions could also be imposed for infringements.

Automated individual decision-making

The General Data Protection Regulation contains rules for automated individual decision-making. These, however, in their current form, unduly disadvantage data subjects. Art. 22(1) GDPR provides for the "right not to be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". In principle, this clause is to be interpreted as a prohibition of automated decisions in individual cases. Art. 22(2) GDPR provides for exceptions to this prohibition if the automated individual decision-making

is necessary for the conclusion of a contract, if it is permissible under the laws of a Member State or if it is based on the data subject's explicit consent. An automated individual decision exists if there has been no human intervention in making a decision. This is the case, for example, if the allocation of seats in an aircraft is exclusively automated, or if an automatically derived score-value is decisive for whether a contract should be concluded or not.

Automated decision-making processes can take into account and process far more information than humans are able to. While they promise better, faster, fairer and more cost-effective results, these procedures also have a high potential for discrimination against data subjects. For example, automated individual decision-making can lead to the rejection of a desired contract or to a higher interest rate being offered than would be the case with optimal creditworthiness. A high potential for discrimination is also expected in the modern world of work. This is particularly the case if automated individual decision-making procedures are used to "sift out" applications according to certain keywords.

It is problematic that the scope of the prohibition of automated individual decision-making is so narrowly formulated and can thus easily be interpreted and applied to the detriment of the person concerned. On the one hand, Art. 22(1) GDPR only covers the decision itself, not the preceding automated processing and thus also not the decision based on automated processing. The provision therefore does not apply if a human takes the final decision. For this reason, the provision is often understood by data processors as not covering cases in which a formal decision is made by a human being downstream, but this human being does not have the practical possibility or sufficient expertise to deviate from the results of the automated individual decision-making. In order to counter this deficit and to make the restrictions on the prohibition of automated decisions in individual cases less disadvantageous for the person concerned, the word "solely" in Art. 22(1) GDPR should be deleted. This would mean that the prohibition would also apply to automated decisions in which a human makes the final decision without being able to influence the content of the decision.

Another restrictive factor is that the law under Art. 22(1) GDPR should only apply if the decision has either legal effects or significantly affects the persons concerned in a similar way. According to recital 71 GDPR, these criteria should include the automatic rejection of an online credit application or automated e-recruiting practices without any human intervention. Art. 22(1) GDPR should therefore not apply to algorithm-controlled direct advertising or the restriction of payment options in e-commerce, insofar as this is automated. To remedy this situation, it should be made sufficient for the right not to be subject to a decision based on automated processing if the processing is likely to significantly affect the data subject in any way.

On the other hand, the prohibition of automated decisions in individual cases does not apply if, pursuant to Art. 22(2)(a) GDPR, the automated decision is necessary for the conclusion or performance of a contract between the data subject and the controller. This exception to the prohibition of automated individual decision-making enables controllers and processors to automate a large part of their decision-making processes at their own discretion. It is questionable why this exception should not apply if the data controller decides that automated decisions by third parties may serve as a basis for their own decisions. This is the case, for example, if a credit assessment is obtained from a third party, which then forms the basis for a decision as to whether a loan should be granted or not. This provision in Art. 22(2)(a) GDPR unilaterally favours the interests of the controller. In order to eliminate this asymmetry, this provision in Art. 22(2)(a) GDPR should be deleted. In this respect, a balance between the interests of the data controller and those of the data subjects could be achieved via the provision, in

Art. 22(2)(c) GDPR, that an exception to the prohibition of automated decisions applies in individual cases, only if the data subject has consented to this form of data processing.

Profiling

A major shortcoming of the General Data Protection Regulation is that, although it mentions profiling selectively, it does not sufficiently regulate its specific risks. Under Art. 21(1) and (2) GDPR, an objection may be lodged against profiling if it serves to protect legitimate interests, in particular direct marketing. Profiling is also prohibited under Art. 22(1) GDPR if it serves as the basis for a solely automated decision – unless one of the exceptions in Art. 22(2) GDPR allows this. All other forms and reasons for profiling remain unregulated in the General Data Protection Regulation.

Profiling is defined in Art. 4(5) GDPR as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

One use of profiling is the evaluation of online usage behaviour. Based on past search queries, search results can be sorted or the evaluation of past purchases can be used for predictive behavioural targeting, product recommendations, pricing or special offers. This means that anyone who uses online services will only see the search results or advertisements that are presumed to be of interest to that person.

However, profiling poses risks to the rights of data subjects that go beyond the normal processing of personal data. For example, price discrimination on the Internet may occur as a result of automated individual decision-making based on a profile, if, for example, customers whose profile (income, interests, preferences) implies a higher willingness to pay are charged a higher price than would be the case without such a profile.

In order to address the specific risks that profiling generates for the fundamental rights of data subjects, risk-appropriate regulation is necessary. The General Data Protection Regulation could explicitly clarify the purposes for which profiling is allowed, and those for which it is not. Similarly to the provision in Art. 9 GDPR for special categories of personal data, the Regulation could stipulate that profiling is, in principle, not permitted and expressly outline the exceptional cases for which the general prohibition does not apply.

Information requirements

Art. 13 and 14 GDPR contain the central information obligations of the controller vis-à-vis the data subject. In comparison to the previous equivalent provisions in the Data Protection Directive, the information obligations in the GDPR have been extended in content. They are, however, in some cases, described in a very abstract manner. The data subject must be provided with all relevant information, including the name and contact details of the controller and the purposes of the processing. A distinction is made according to whether personal data are collected from the data subject or from a third party.

If the personal data is collected from the data subject, the information pursuant to Art. 13(1) and (2) GDPR must be provided immediately at the time of collection. In practice,

this is often understood to mean that when a contract is concluded or when the data subject is first contacted, all conceivable eventualities of future data processing must be described in comprehensive data protection declarations or general terms and conditions. This is often done long before the data is actually collected and before the data subject decides whether or not he or she agrees to the data processing. As a result, the data subject will not remember the comprehensive content of the information provided – which may have been provided years in advance – when their data is (at some point) actually collected. The practice is thus not in line with the objective of the General Data Protection Regulation to inform the data subject in such a way that he or she can exercise his or her informational self-determination in the best possible way, and thus with the requirement of Art. 13(1) GDPR to inform data subjects at the time of collection.

To ensure that the purpose of the duty to inform is not nullified, additions to the wording of Art. 13(1) and (2) GDPR are necessary to clarify that the information should be provided in a manner appropriate to the situation, namely immediately before the concrete data collection and the potential decision of the data subject. Art. 13 and 14 GDPR differ in content with regard to the time of information and the scope of the exceptions of the duty to inform. A collection of data from third parties deprives the data subject of the opportunity to obtain information about the data processing and to influence this processing if the controller does not specifically name the sources of the data, and does not make these transparent from the outset. To remedy this shortcoming, Art. 14 GDPR should make the provision of this information mandatory.

Right to data portability

The right to data portability is a prominent novelty of the new data protection law. It gives the data subject the right to transmit, or have transmitted, data that he or she has provided to the controller to another controller. This provision, which is aimed particularly at social networks, is intended to reduce so-called lock-in effects and increase competition between providers.

The article's title is misleading. Instead of "data portability" it should be called "data transmission", since it encompasses the right to have personal data transmitted and is not intended to establish only the theoretical possibility of the transmission, which is indeed suggested by the wording used (the ability of data portage). The benefit of this right for consumers is limited by three problems caused by the text of the Regulation.

First of all, the term "provided" in Art. 20(1) GDPR is not clear enough and is interpreted in different ways in practice. In order to achieve meaningful results, the term should be replaced, for example, by "prompted" or "caused". To date, the scope of what is considered "provided" within the meaning of the provision is controversial and is restricted by the controllers to the detriment of the persons concerned. In order to effectively guarantee the right to data transmission, the right should include both data provided by the data subject – in the sense of active input – as well as all data generated by the use of the system or device, such as a search history, playlists, traffic and location data, fitness data, but also data of third parties which the data subject may lawfully have at his or her disposal, such as a chat history. Ultimately, the aim is to demarcate spheres of influence between the data controller and the data subject and to appreciate the data subject's contribution in the creation of the data. The data subject's power of disposal is derived from his or her contribution to the creation of the data. If the data subject has caused the data to be created but the controller has contributed little to this, for example, by merely providing the infrastructure, the data created should also be under the control and use of the data subject. This logic makes it clear that Art. 20 GDPR must also be extended to raw data caused by the data subject's conduct.

According to Art. 20(1) GDPR, the right to data transmission exists only if the processing is based on consent pursuant to Art. 6(1)(1)(a) or Art. 9(2)(a) GDPR or on a contract pursuant to Art. 6(1)(1)(b) GDPR. The question as to whether this right still exists when consent is revoked or a contract is terminated, is not clarified. Without consent or without a contract, the data must be deleted in accordance with Art. 17(1)(a), (b) or (d) GDPR. Following such a deletion, data transmission would then no longer be possible. The provision could be read in the way that data transmission is still possible even subsequent to the termination of validity of the legitimation of processing, as long as the controller has not yet deleted the data. However, a clarification of the text is necessary here. In this regard, it could further be stipulated that the right would need to be asserted within an appropriate time period after a revocation of consent or a termination of a contract.

Finally, the wording is unclear as to the forms in which the data subject may request the data transfer. The provision is characterised by undefined legal terms such as "commonly used", "machine-readable" and "structured", which are interpreted in a highly inconsistent manner by the controllers, and which lead to inappropriate results to the detriment of the data subject. Specific formats are not specified. Recital 68 GDPR is not helpful either which states that the right of the data subject to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Interoperability – mentioned only in passing in recital 68 GDPR – would mean that data might only be transmitted in a format that allows another controller to process it. This is where a legal anchoring would be appropriate. In any case, it would be advantageous if the European Data Protection Board were to lay down specific technical conditions for interoperability.

Conceptual deficits of the GDPR

In addition to the practical deficits discussed above, the General Data Protection Regulation has other, sometimes serious, conceptual deficits. These latter deficits are likely to result in the General Data Protection Regulation failing to achieve the goals it has set for itself, namely to harmonise data protection law throughout the European Union, to offer uniform requirements for equal economic conditions in the European Union and thus to strengthen the internal market and, finally, to contribute to the modernisation of EU data protection law.

A central problem of the General Data Protection Regulation lies in the large discrepancy between the high complexity of the need for regulation on the one hand, and the abstractness of provisions on the other. With only 51 material provisions, the GDPR attempts to meet the challenges of data protection law, for which, in some Member States, thousands of sector-specific regulations existed prior to the applicability of the GDPR. Accordingly, the sometimes highly abstract provisions of the General Data Protection Regulation create a high degree of legal uncertainty among the addressees.

The General Data Protection Regulation fails to achieve its objective of harmonising data protection law throughout the European Union because, despite its primacy of application, it must leave implicit and explicit leeway for Member State rules to do justice to the complexity of its subject matter. This freedom consequently leads to the fact that the provisions of the General Data Protection Regulation are concretised, specified or supplemented in different ways in the Member States and are interpreted in accordance with the respective national data protection culture to date (e.g. with regard to Art. 6(1)(1)(f) GDPR). Although the supervisory authorities coordinate their legal opinions on a wide range of issues in the European Data Protection Board, this alone does not guarantee a uniform interpretation of data protection law, especially as the courts in the Member States are not bound by these opinions. Due to the different concretisations and specifications of the provisions of the General Data Protection Regulation in the Member States, the General Data Protection Regulation also fails in its goal to set equal economic conditions across the European Union.

Nor does the General Data Protection Regulation meet the objective of modernising data protection. With few exceptions, it fundamentally upholds the concepts elaborated in the 1995 Data Protection Directive and, for this reason alone, cannot meet the current and future challenges posed by information and communication technologies.

For example, it adheres to data protection principles that largely date from a time even before the Directive, when neither PCs nor the Internet existed. However, in times of ubiquitous computing, big data, adaptive algorithms and the recording of the world by artificial intelligence systems, these principles are coming under massive pressure, which casts doubts on their future applicability. For example, the principle of purpose limitation is being undermined by smart car, smart home and smart health applications, as these applications require the broadest possible databases on user behaviour, interests and preferences in order to best support the user. The actual goal of purpose limitation, namely to limit data processing to the extent necessary, is thereby thwarted by the idea of unnoticed, complex and spontaneous technical support and by the goal of gaining new insights by combining and evaluating as much data as possible from a wide range of sources.

In turn, a system design in which private individuals can carry out processing operations as part of an infrastructure (e.g. blockchain, mix networks, crowd sensing, peer-to-peer communication) is not addressed in the General Data Protection Regulation. In these

cases, the limits of responsibility are not clear or could unduly disadvantage the private parties involved. Furthermore, an advancement of the General Data Protection Regulation in terms of collective aspects, including rights management, should be considered.

It should also be possible to hold manufacturers more accountable. This is particularly true with regard to the requirement of data protection by design and by default (Art. 25 GDPR). Currently only the controller is the addressee of the provision and it is incumbent upon the controller to demand that processors, manufacturers and service providers implement the principle. In practice, however, this has had little visible effect and the good idea of built-in data protection still falls far short of its potential.

Another example is the requirement for transparency, which is subject to subjective and objective limits due to current and future information and communication technologies. Subjectively, the expected multiplication of data processing in all areas of life exceeds, by orders of magnitude, the human attention required to make transparency effective. Objectively, high complexity, multiple purposes and adaptive systems set narrow limits to the degree of transparency possible. In order to meet current and future challenges raised by information and communication technologies, new, complementary and more precise data protection principles are required.

The General Data Protection Regulation also misses its modernisation objective due to its specific approach to technological neutrality. The approach of technological neutrality makes sense insofar as it has the effect that legal provisions are formulated in such a way that they do not exclude further technical developments. However, the General Data Protection Regulation uses this approach in the sense of risk neutrality, i.e. not a single legal ground for processing addresses the particular fundamental rights risks engendered by modern information technology, such as smart information technology in everyday life, big data or cloud computing. The provisions of the General Data Protection Regulation apply equally to the customer list at the "bakery around the corner" and to the data processing operations of major global corporations, which pose much graver risks to data subject' rights. It is precisely this circumstance that threatens to cause considerable acceptance problems with regard to the General Data Protection Regulation on the part of the European population – and thus scepticism about the policies and legislation of the European Union as a whole. Art. 6 of the eCall Regulation (EU) 2015/758, which sets clear data protection requirements for the admissibility of automated emergency calls, demonstrates that it is perfectly possible to provide for technology-neutral as well as function- and risk-specific data protection regulations in Union law.

The risk-neutral "One Size Fits All" approach pursued by the General Data Protection Regulation makes sector-specific concretisations and additions to data protection law indispensable in order to be able to react appropriately to the challenges of modern information and communication technologies. Various actors can be considered for the necessary concretisations and additions: the European Union legislator, who can issue sector- or technology-specific European regulations or directives; the Member States, who can supplement and concretise the Regulation within the national scope accorded by the General Data Protection Regulation; the European Data Protection Board, which can publish guidelines and recommendations; the national supervisory authorities, which can support all those involved with guidelines, in particular on the correct handling of the innovations of the regulation; and private actors (such as economic associations or standardisation organisations), which can draw up sector-specific codes of conduct.

Summary and conclusions

The General Data Protection Regulation has improved the position of data subjects with regard to the processing of personal data. However, it still falls short of its potential in many areas. As a consequence of its sometimes abstract requirements, its provisions are open to being interpreted in such a way as to restrict data protection. Due to the abstract nature of its standards, there is a risk that the addressees of these standards will use this scope to the detriment of data subjects. For this reason, this policy paper makes proposals for constructive further development of the Regulation, which can be used in the evaluation of the General Data Protection Regulation in 2020.

In preparing the proposals, the focus was on data subjects. Strengthening their position and reducing power asymmetries between providers and data subjects is in line with the intended objective of the General Data Protection Regulation – to place the processing of personal data at the service of humankind and to safeguard the rights and freedoms of data subjects, while at the same time taking into account the interests of data processors. The investigation has shown that even small changes to the wording of the standard text of the General Data Protection Regulation could lead to a significant improvement in data protection and legal certainty for all stakeholders.

Where minor changes to the wording of the Regulation are not possible, Member State legislators, the European Data Protection Board, national data protection supervisory authorities and private actors, in particular, must take action in addition to the Union legislator to concretise the undefined requirements of the General Data Protection Regulation.

The task of further developing data protection does not conclude with the upcoming evaluation of the General Data Protection Regulation in 2020. The discourse on data protection law must not be allowed to stand still in view of the high pace of transformation and innovation in the field of data processing. The basic principles of data protection in the European Union have remained largely unchanged since the 1970s. Innovations in information and communication technologies that have already been realised since then, or are foreseeable in the future, make it necessary to continually question these basic principles and to develop them further.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein