Roßnagel, Alexander; Bile, Tamer; Friedewald, Michael et al.

Book

National implementation of the General Data Protection Regulation : challenges - approaches - strategies : policy paper

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVACY AND SELF-DETERMINED LIFE IN THE DIGITAL WORLD

Policy Paper

NATIONAL IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION

CHALLENGES – APPROACHES – STRATEGIES

IMPRINT

Authors:
Alexander Roßnagel, Tamer Bile, Michael Friedewald, Christian Geminn, Olga Grigorjew, Murat Karaboga, Maxi Nebel

Contact:
Michael Friedewald

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

Fraunhofer-Institut für System- und Innovationsforschung 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, January 2018

Outline

With the General Data Protection Regulation (GDPR, the Regulation) taking effect on May 25th 2018, data protection in Europe will receive a new foundation. This essential reform has three major goals: a unionwide harmonisation of data protection law, an equalisation of competition and a modernisation of data protection law.

The change from the instrument of a directive to a regulation has far-reaching consequences. It makes it necessary to extensively adapt and adjust national law. Since there is no primacy of validity, established national provisions remain in effect, but due to the primacy in application of the Regulation they must not be executed, if they contradict the Regulation.

Genesis of the GDPR

Almost all areas of life, economy and administration depend on processing personal data and anyone who decides on the execution and interpretation of data protection law wields a pivotal instrument for the design of the digital economy and society in the European Union. Since the Member States have been unable to achieve a sufficient harmonisation of data protection law with a high, union-wide data protection standard based on the Data Protection Directive, the European Commission proposed a new solution for the necessary modernisation of data protection law in 2012. By choosing the instrument of regulation, the Member States were supposed to be excluded from enacting further data protection law to a large extent. Their – at least in some Member States – very differentiated and risk-oriented provisions concerning data protection were supposed to be replaced by few abstract and general provisions. At the same time, the Commission had retained the right and responsibility to decide which measures would be necessary and beneficial to promote data protection beyond these provisions by adopting implementing act and delegated acts.

This concentration of legislative power at the hands of the Commission was prevented by the European Parliament and by the Council. At the end of the trilogue, out of all the powers that the Commission had envisioned for itself, only two for adopting delegated acts and seven for adopting implementing acts remained. While the Parliament's draft was hallmarked by a terminal and detailed design of provisions which were left abstract and indeterminate in the Commission's draft, the Council was able to successfully push toward a regulation whose abstract provisions can to a significant extent be customised or which allows the Member States to maintain specific data protection provisions or enact new provisions. Ultimately, the political and temporal pressure in the trilogue has prevented a coherent framework on data protection from emerging – a result that could have been avoided by further deliberations.

Shortcomings of the GDPR

Since the regulation is kept abstract and leaves significant room for deviations by the Member States, it puts the goal of a union-wide harmonisation of data protection law into peril.

Harmonisation

The demands for a union-wide data protection law are highly complex. The Regulation misjudges this. The provisions of the GDPR exhibit a great degree of abstraction and thus lack complexity. Within just 51 articles of substantive data protection law, the Regulation aims to address the same issues for which in some of the Member States thousands of sector-specific provisions have been created (e.g. in Germany). Data pro-

tection has become a pivotal cross-sectional issue of the information age. Automated processing of personal data affects all areas of life. All processes in administration, economy and culture are shaped by it. The Regulation's attempt to replace the enormous number and bandwidth of data protection provisions in 28 Member States with only 51 substantive provisions does not do justice to the scope of the matter.

However, a complete replacement of national data protection law is not part of the structure of the GDPR. On the contrary, its abstract provisions are very much in need of amendment and specification. The Commission wanted to adopt the amendments itself; Parliament wanted to integrate them into the text of the Regulation. The Council wanted the Member States to step in. It was this approach that prevailed. For this reason, the Member States are now left with comparatively broad room for manoeuvre, within which they can specify indeterminate terms and concepts, concretise and amend incomplete provisions or fill gaps in the Regulation – albeit having to be careful not to go against the objectives of the Regulation. On top of this, there are the regulatory mandates and options within the Regulation. Existing national provisions can thus remain applicable and new provisions can be created.

Meanwhile, deficits in clearing up national law may lead to significant legal uncertainty. The European Union has neither the authority to change or override national law, nor is there a primacy of validity of Union law. This means that without national lawmakers becoming active, existing national data protection provisions will continue to be valid. In case of a conflict between Member State law and Union law, the application of the GDPR takes priority.

Consistent data protection practice

Where the GDPR and not Member State law is applicable, this may also sometimes lead to an uneven playing field within the European Union. In practice, the abstract and indeterminate provisions of the Regulation have to be concretised by the national supervisory authorities and by the courts. Indeed, the European Data Protection Board (EDPB, the Board) is tasked with ensuring the consistent application and issuing appropriate guidelines, recommendations, opinions and best practices. These, however, only bind the supervisory authorities and do not establish generally binding executive law. The interpretations of the Regulation can differ between the supervisory authorities; the review of these interpretations is up to the local courts. Different opinions between the courts can prevent any attempt of a consistent interpretation of the Regulation. This means that consistent case law may only be achieved by the European Court of Justice (ECJ) – and even then only concerning individual questions after long trials.

In addition to this, the harmonisation of data protection law within the Union and with it legal certainty is endangered because of provisions like Art. 6(1)(1)(f) GDPR. The weighing of legitimate interests of the controller on the one hand and the interests or fundamental rights and freedoms of the data subject on the other hand will most likely be performed in accordance with the established national culture of data protection. In practice this will lead to different results in application and execution of the GDPR in the individual Member States. Subsequently, for example in the context of weighing interests with regards to CCTV there will be different concretisations in the Member States, depending on how CCTV was regulated in the past. Other examples, where the weighing of interests is likely to have different outcomes depending on the established practice of a Member State, are advertising, market research and credit agencies. The lawfulness of processing will have a different yield in each Member State which prevents a union-wide data protection law from forming. A level playing field, thus, cannot be achieved.

The issue is intensified by the fact that it is the courts who are deciding on the weighing of the relevant interests. This may lead to even less harmonisation than under the

Data Protection Directive. It will ultimately be possible that the results of balancing interests will differ from circuit to circuit, even within a single Member State like Germany where in the past the standardisation of the balancing has been made by the legislator and thus has been consistent. In a position to give legal clarity on how to correctly balance interests in certain cases are the higher courts in each Member State and the ECJ. However, such decisions can take a very long time.

Modernisation

The third target of the GDPR – to modernise data protection and equip it to deal with the challenges of the future – is also missed in many places. There are two main reasons for that: With a few exceptions, the Regulation continues the conceptual design of the Data Protection Directive and thus ties in with solutions that were incorporated in European law more than 20 years ago and which even then were partially considered to be out of date or insufficient. For this reason, the Regulation does not meet the upcoming challenges of technological and economic development. Holding on to outdated and inadequate solutions is particularly impactful because Member States cannot deviate from these fundamental concepts set forth by the Regulation.

With regards to content, the Regulation does not achieve significant modernisation because it has a very specific approach to technological neutrality. Technological neutrality means to prevent legal provisions from excluding technological innovation or from becoming obsolete because of their wording. Therefore, technological neutrality avoids naming specific constitutive criteria and limits itself to the regulation of technological functions which are not tied to a specific design. The approach of the Regulation, however, is not to regulate any technological risks whatsoever. This means that its provisions on the lawfulness of processing, the rights of the data subject and on protective measures are risk-neutral. In none of its provisions does the Regulation address the specific risks of modern information technology to fundamental rights and freedoms or present solutions to deal with these risks. Such risks result specifically for instance from ubiquitous computing, the Internet of Things, Big Data, Cloud Computing or data-driven business models, automation, Artificial Intelligence and self-learning systems. Furthermore, the Regulation does not differentiate between forms and scopes of data processing. The provisions on the lawfulness of processing, purpose limitation and rights of the data subject apply to all controllers in equal measure – may it be the small local business just around the corner which maintains a short list of customers or big corporations like Google or Facebook which process massive amounts of personal data with high-risk technological systems. Such provisions will not be able to address the specific risks to fundamental rights and freedoms. However, Art. 6 of the eCall Regulation (EU) 2015/758 or Art. 8, 10 and 16 of the Commission draft for an ePrivacy Regulation show that this is perfectly possible in Union law.

Co-regulation, regulatory mandates and options

Ultimately and in contrary to initial expectations, the GDPR establishes a co-regulation between the European Union and the Member States. It stipulates the goals and fundamental principles, basic rights and duties as well as the fundamental structures of the enforcement of data protection within the European Union, but in many cases it leaves the specification and amendment of these provisions to the Member States. For this purpose, the Regulation contains numerous opening clauses for the Member States to utilise. These opening clauses can be categorised as regulatory mandates and regulatory options. The latter are those which entail the aforementioned risks, but also significant opportunities.

Co-regulation, regulatory mandates and options

Regulatory mandates are opening clauses which obligate the Member States to adopt certain provisions. Examples are Art. 51 et seq. GDPR on providing an independent supervisory authority, Art. 84 on further penalties and Art. 85 GDPR on securing freedom of expression and information.

In contrast, regulatory options are opening clauses, which allow the Member States to create their own provisions or to maintain existing provisions, if these provisions do not conflict with the Regulation. Such clauses are Art. 6(2) and 6(3) GDPR on data processing carried out in the public interest. According to Art. 9(2)(a), (b), (g), (h), (i) and (j) as well as 9(4) GDPR Member States may regulate the processing of special categories of personal data. Art. 23 GDPR allows for restrictions of the rights of the data subject in certain circumstances. Other examples are Art. 37(4), 80(2), 88 and 89 GDPR.

The regulatory options in particular bear the risk of legal uncertainty, since they may lead to a complex and intransparent situation in which it becomes difficult for controllers and data subjects to discern which provisions are relevant to them. They also hamper the harmonisation of the legal framework in the Member States. They can, however, be used not only to take into account national characteristics, but also to create a legal framework that is risk-adequate. Only then, the necessary complexity of data protection provisions can be achieved in the face of society-wide processing of personal data. The range of the regulatory options is unclear in certain cases, particularly because of their abstract and superficial provisions. For a start, Member States must begin to experiment taking advantage of the regulatory options.

A regulation which addresses the difficult issues of data protection law conclusively or a directive which creates a clear division of tasks between Union and Member States would have been preferable to the current situation. But due to the fact that a monopolisation and centralisation of the advancement of data protection law was prevented, the current situation at least offers the chance to test the possibilities of a meaningful division of tasks and responsibilities between the Union and the Member States. In the face of the diversity and dynamics of future and yet unknown challenges of information technology and its application to fundamental rights, the Regulation in the form in which it has become law enables the Member States in many places to experiment with different regulatory concepts. This way, a number of sources can contribute to a vivid data protection within the Union. Instead of a uniform data protection practice, indeterminate legal terms and their situational concretisation make it possible that in the individual Member States data protection can be adapted to the local requirements. And ultimately, the manifold regulatory options offer the Member States a chance for a modernisation of data protection law by seeking to guarantee an adequate protection of fundamental rights and freedoms against future challenges via the creation of risk-adequate provisions.

Relating to the regulatory option mentioned above, it is the responsibility of the Member States to ensure legal certainty and fairness as well as enforceability and effectiveness of data protection. To fulfil this responsibility, there are three possible concepts:

- The minimal solution fulfils the regulatory mandates, continues existing provisions to a limited degree and maintains the existing national data protection level in the Member State.
- The maximal solution fulfils the regulatory mandates, but also makes use of both the regulatory options as well as implicit possibilities for regulation in order to achieve increased legal clarity, risk-orientation and a reduction of effort.
- The – arguably – optimal solution attempts (in the face of high pressure of time) to fulfil the regulatory mandates and to adopt provisions which on the one hand ensure the enforceability of the major requirements of the Regulation and to eliminate deficiencies, but on the other hand are less disputed. Provisions with a heightened need for counselling are postponed. Where there is doubt, existing provisions are maintained until after May 2018.

Besides these approaches to coherent and strong data protection legislation there is, however, the risk that Member States will use their room for manoeuvre to lower the level of data protection.

Implementation of the GDPR

In order to ensure legal certainty, enforceability and effectiveness of the Regulation, the provisions of the Regulation must be accompanied by national provisions in the Member States. The Regulation consequently leaves implicit and explicit regulatory scope for Member State lawmakers. The Member States can utilise this scope in different ways.

Further application of Member State provisions

Firstly, the Member States can specify abstract provisions of the Regulation and thus provide standards of evaluation and for action which the Regulation lacks. Such specifications are only permissible as long as they do not contradict the Regulation. A contradiction exists, where a national provision violates the regulatory goal of the Regulation. If only an indeterminate legal term is specified whose specification is not reserved for a certain actor, then this specification can be used to support the Regulation – even if the wording differs from the Regulation.

Secondly, Member States can substantiate and amend the Regulation with national provisions which make an incomplete provision of the Regulation enforceable in the first place. This is particularly the case where in the original draft the Commission intended to introduce delegated and implementing acts, which then were omitted without any kind of replacement. Then the completion and amendment of incomplete provisions as well as the closing of regulatory gaps enable the execution and enforcement of the Regulation by the supervisory authorities and the courts. The same applies where national provisions create the necessary regulatory framework for the execution of the the Regulation or where a national provision adapts the Regulation to the national systematics and the national use of language.

And thirdly, Member States can make use of any of the 70 opening clauses of the Regulation which gives the Member States room for manoeuvre to apply their own national provisions in accordance with Union law or to create new provisions. Such opening clauses for entire sectors are contained in chapter IX on provisions relating to specific processing situations (Art. 85 to 91 GDPR). In many cases, opening clauses exist in order to enable the adapting of provisions of the Regulation to the specific circumstances in the Member States – for instance in Art. 9 and 23 GDPR.

Examples of the implementation of the GDPR

Germany and Austria are the first Member States to pass laws on the implementation of the GDPR and on the adaptation of national data protection law. Germany passed its new "Bundesdatenschutzgesetz" (BDSG, Federal Data Protection Act) in May 2017. The new Austrian "Datenschutzgesetz" (DSG, Data Protection Act) was promulgated in July 2017. Both come into force on May 25th 2018.

It has to be noted that Austria was the only Member State to vote against the adoption of the GDPR in the Council in April 2016, citing unresolved issues combined with the expectation that these important issues could not be offset by the Member States because of the nature of a regulation.

The following examples demonstrate if and how German and Austrian lawmakers have used their room to manoeuvre.

Amending the Regulation

The German legislator has fulfilled the explicit regulatory mandates of the GDPR: An important example of this are amending provisions for a consistent enforcement of the Regulation with regard to the cooperation of supervisory authorities, the consistency mechanism and representation in the EDPB. Such provisions are necessary, because the Regulation has tasked the supervisory authorities with ensuring consistent execution and enforcement of the Regulation as well as with many aspects of the execution itself. The German legislator has accomplished this explicit regulatory mandate by regulating Germany's representation in the Board and the decision-making process among the supervisory authorities in Germany's federal system (§§ 17 to 19 BDSG).

In Austria, such provisions were not necessary because it maintains only one supervisory authority.

The Regulation also implicitly requires further provisions to achieve its goals. However, any of these requirements were not acted upon with the new BDSG. The new act lacks provisions that determine when a data protection impact assessment according to Art. 35(10) GDPR has to be carried out where processing occurs pursuant to Art. 6(1)(1)(c) and (e) GDPR. There should also be a provision that regulates when to repeat a data protection impact assessment. The provisions on codes of conduct in Art. 40 GDPR lack amending provisions on the process of development that ensure a minimum of fairness and consideration of interests as well as provisions on the participation of relevant stakeholders, on the degree of the compulsion of approved codes of conduct and on the time limit of the approval. The certification of "processing operations" (Art. 40 GDPR) require for instance provisions on what a „transparent" process according to paragraph 3 entails and on which information is "necessary" according to paragraph 6. The cooperation with supervisory authorities of other Member States according to Art. 60 GDPR, mutual assistance and joint operations also require amending provisions.

Such implied but non-mandatory amendments which would contribute to an increase in the level of data protection have neither been adopted in Germany nor in Austria.

Specifying the Regulation

The German legislator has made specifications for instance in § 1 BDGS with regard to Art. 2 GDPR, in § 2 with regard to public and non-public bodies as controllers in accordance with Art. 4(7) GDPR, in § 19 with regard to lead supervisory authority (Art. 60 GDPR) as well as in § 22(2) with regard to the terms "appropriate safeguards" or "suitable and specific measures" as mentioned in Art. 9(2)(b), (g) and (i) GDPR.

The Austrian legislator for instance has specified the term "controller" (Art. 4(7) GDPR). In contrast to the German implementing act, the Austrian act, however, contains no specifications with regards to "appropriate safeguards" or "suitable and specific measures".

Similar specifications would also be helpful in the context of the rights of the data subject, for instance with regard to "appropriate measures" to provide information to the data subject (Art. 12(1)(1) GDPR), and in the context of the responsibility of the controller, for example with regard to "appropriate technical and organisational measures" (Art. 24(1) GDPR). However, neither the German nor the Austrian legislator has adopted such provisions.

With regard to codes of conduct and certification it should be specified how to promote them and how to factor in the interests of small businesses. The same applies for the responsibilities of the processor in order to increase legal certainty.

Specifications are also necessary with regard to the indeterminate legal terms in Art. 32 GDPR. It is currently unclear what "resilience of processing systems" in Art. 32(1)(b) GDPR entails. Art. 32(1) GDPR lists examples of providing data security. This list is not

exhaustive. Therefore, Member States are free to adopt additional requirements for data security as long as they do not contradict the Regulation.

It would also aid legal certainty, if abstract provisions like Art. 36(1) GDPR were specified, which requires prior consultation with the supervisory authority if there is indication "that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk". It would have helped to set criteria for what constitutes a "high risk" in order to give controllers guidelines on how to evaluate the situation. The new Data Protection Act does not contain such guidelines.

The last examples to mention are the tasks of the supervisory authorities in Art. 57 GDPR and their powers in Art. 58 GDPR. The Regulation sets out a broad range of tasks and powers for the supervisory authorities and leaves Member States little room for adjustment. However, many provisions require concretisation, specification and amendment. The German legislator has taken such action only sporadically, notably with regard to the division of responsibilities in the federal system and with regard to accreditation.

The Austrian legislator was more even reluctant and regulated the tasks and powers of the national supervisory authority in § 21 et seq. DSG to a far lesser extent.

Use of opening clauses

German lawmakers have used the possibilities presented by the many opening clauses of the GDPR rather one-sided. In many cases, the new national provisions are not limited to adapting national law to the Regulation, but set their own accents by adjusting provisions of the Regulation and of the previous Federal Data Protection Act. They are characterised by shifting the weighing of interests in favour of the controller and at the expense of the data subject. This is particularly evident when it comes to the restrictions of the rights of the data subject in §§ 32 to 37 BDSG pursuant Art. 23 GDPR.

§ 32 BDSG for instance limits the duty to supply information where personal data are collected from the data subject. If a public authority intends to further process personal data for a purpose other than that for which the personal data were collected, it does not have to provide information about this if doing so would endanger the proper fulfillment of a task that the public authority has to carry out as long as that task is listed in Art. 23(1)(a) to (e) GDPR. Furthermore, the interests of the controller for not issuing the information have to outweigh the interests of the data subject. Further restrictions on the obligation to provide information and the right of access can be found in §§ 33 and 34 BDSG.

The right to erasure according to Art. 17 GDPR has been limited by the German legislator in § 35 BDSG at the expense of the data subject. This particular right of the data subject does not apply for instance if erasure is only possible with disproportionate effort and the interest of the data subject with regard to erasure is low. The right to object (Art. 21 GDPR) does not apply in relation to a public authority, if there is an imperative public interest in the processing which outweighs the interests of the data subject or if processing is mandatory according to the law.

Additionally, according to § 37 BDSG the right not to be subject to a decision based solely on automated processing (Art. 22 GDPR) does not apply, if the decision is made in the context of an insurance contract and the request of the data subject is granted.

The German legislator has taken advantage of the opening clause of Art. 88 GDPR concerning processing in the context of employment and carried over the provisions of the old Data Protection Act with only minor changes. Likewise, the Austrian legislator has used Art. 88 GDPR to refer in § 11 DSG to the existing regulations in the Arbeitsverfassungsgesetz (Labor Relations Act).

In contrast to the German legislator, the Austrian legislator has made use of the opening clause of Art. 8(1) GDPR. According to § 4(4) DSG, a child can give consent if it is at least 14 years old, thus deviating from the threshold set by the Regulation.

Furthermore, the Austrian legislator has made use of the opening clause in Art. 85(2) GDPR which allows the Member States to reconcile the right to the protection of personal data with the freedom of expression and information (§ 9 DSG).

The example of CCTV surveillance shows, which mistakes Member States should avoid in order to prevent their newly enacted provisions from being declared incompatible with Union law by the ECJ. Germany and Austria have kept or enacted extensive provisions on the lawfulness of video surveillance and have overshot the mark in that regard. The Regulation conclusively regulates in Art. 6(1)(1)(a) to (f) GDPR the lawfulness of processing. Art. 6(2) GDPR allows the introduction of more specific provisions by the Member States only with regard to Art. 6(1)(1)(c) and (e) GDPR. Germany and Austria, however, have adopted extensive provisions on video surveillance for instance with regard to domestic authority and the interests of private controllers. The Member States have no authority to regulate the lawfulness of private data processing. Furthermore, these national provisions are incompatible with Union law as far as they disregard fundamental principles of European law (for instance primacy of application and the ban of repetitions). Other Member States should thus pay close attention to the provisions of the GDPR.

In order to meet the challenges of modern data processing, Member States should use the individual opening clauses – for instance in the context of employment and in the public sector – to create risk-adequate provisions as a basis for lawful processing. This entails requirements for the design of IT systems in a specific area, which would enable transparent and sparing processing of personal data, prevent the creation of profiles and the unnecessary localisation of employees and limit processing to anonymous or pseudonymous data if possible. In addition, conditions for lawful deanonymisation in certain limited cases should be set, as well as provisions on purpose limitation and purpose binding and processing on behalf of the controller. Since the processing of anonymous data can also endanger informational self-determination, the processing anonymous data should also be subject to certain principles. Furthermore, requirements for data security as well as measures on self-data protection by the data subject should be specified. Specifications on effective consent and on the weighing of the interests of the data subject and of the controller continue to be essential to lawful processing of personal data. Specific provisions are also necessary with regard to the lawfulness of profiling and the circumstances of the processing of special categories of personal data. With regard to the rights of the data subject, specifications on the duration of storage and the obligation to erase should be devised.

Conclusions

The Regulation misses several of its targets and does not contribute to a systematic, comprehensive and uniform restart of data protection law in all Member States of the Union. Instead, it leads to a co-regulation and cohabitation of Union law and national law. This creates a number of difficult legal questions on how these fields of law will interact and which law will apply in the future. In the face of these open questions, legal uncertainty arises for both controllers and data subjects.

The opinions etc. of the Article 29 Working Party and the guidelines etc. of the EDPB can make a significant contribution towards increasing legal certainty. They help create and secure a consistent interpretation of Union law. Furthermore, legal certainty could be increased significantly if the ECJ went beyond answering individual questions more frequently and instead took a stand on fundamental issues.

The Member States can confront legal uncertainty by adapting their general and sectoral data protection law to the Regulation or by evolving it. However, instead of going beyond the scope of protection provided by the existing German Federal Data Protection Act, Germany as the first Member State to implement the GDPR has opted to lower the national standard effectively, in some places even below the standard provided by the GDPR. Austrian lawmakers have also passed on the chance to modernise data protection law and left much of the scope for initiative provided by the GDPR unused. It seems that the goal was to merely fulfil minimum requirements of the Regulation instead of setting a higher data protection standard.

A thorough revision of the GDPR and with it of the fundamentals of European data protection is unlikely to occur in the foreseeable future. However, the European Union can regulate sectoral and technologically specific data protection. Good examples are Art. 6 of the eCall Regulation (EU) 2015/758 and the draft of the proposed ePrivacy Regulation. In the latter, the Commission deviated from the technological neutrality of the GDPR and does not apply the general rules of the GDPR, but instead creates risk-specific provisions to regulate the particular technologies of electronic communication. Should the Commission decide to create further sectoral provisions, then that would be a step in the right direction.

However, the Union will only set out to create modern, risk-specific provisions, if the relevant stakeholders put on sufficient pressure. A suitable tool to reach this goal would be exemplary provisions created by the Member States which in particular amend or specify the abstract and incomplete provisions of the GDPR. The Member States should make use of the more than 70 opening clauses that the GDPR contains. In this context, the German Conference of the Independent Data Protection Authorities has called upon the Member States to use the opening clauses for modernising data protection law. Nevertheless, the EDPB in particular should make use of its extensive authority to contribute to both a harmonisation of and an increase in the data protection standard. The Board should work towards a prompt union-wide agreement and understanding particularly with regard to difficult questions and provide solutions to both the Member States and the users on how to create modern and consistent data protection.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

PROJECT PARTNERS

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