The General Data Protection Regulation: From a Data Protection Authority's (Technical) Perspective

For the first time, technical data protection plays a major role in privacy law with the enactment of the General Data Protection Regulation (GDPR). A number of obligations for controllers and the rights of data subjects in the GDPR refer to technical aspects. From a data protection authority's technical perspective, in this article, the challenges and open questions that persist one year after the application of the GDPR are discussed.

The General Data Protection Regulation (GDPR) has introduced new obligations for parties that process personal data (so-called controllers) and new rights for natural persons whose personal data are being processed (so-called data subjects). It is the duty of data protection authorities (DPAs) to check whether controllers are in compliance with the GDPR and to help data subjects accomplish their rights. Before the enforcement date of the GDPR (25 May 2018), the high fines implemented as part of the GDPR were the focus of attention. The public expected that from then on, companies would need to take privacy protection seriously (for the first time), as it could cost them a fortune if they were not in compliance with the GDPR. The DPAs, which had been seen as "toothless tigers" in the past, have now gained the confidence and importance necessary to enforce the GDPR in Europe and (preferably) the rest of the world.

In most European countries, there is only one national DPA responsible for the private and public sector of that country, whereas in Germany there are 18 DPAs: one federal and 17 state DPAs for 16 states (in Bavaria, there is one DPA for the private sector and one DPA for the public sector). All of those DPAs are independent from each other. The Commissioner for Data Protection and Freedom of Information Baden-Württemberg is the responsible DPA for the state of Baden-Württemberg (BW) and its 11 million inhabitants. Aside from being responsible for the public sector, the BW-DPA is responsible for nearly 400,000 companies in Baden-Württemberg. Among those companies are world leaders in car manufacturing, automation, and engineering, making Baden-Württemberg one of the wealthiest regions in Europe. Thus, the BW-DPA has a leading role with regard to the private sector, and my experience, which is presented in this article, is also transmissible to other DPAs in Germany and Europe.

Technical data protection, i.e., "the compliance with privacy law by employing technical means," has gained importance since the enactment of the GDPR not only with a new requirement for privacy by design (PbD) but also with a requirement for security of processing, violations now punishable by a fine for the first time (in Germany). Despite that fact, computer scientists still play a minor role in DPAs: For instance, among its roughly 60 employees, only one computer scientist, in addition to three other employees with technical backgrounds, work for the BW-DPA. This means that the sole person with technical expertise at the BW-DPA is responsible for approximately 100,000 companies. A 2015 survey among German DPAs revealed similar numbers of people with technical backgrounds working for DPAs, and since that time, the number has not increased significantly for other DPAs. The number of companies for which the sole person with a technical background is responsible in the

economically strong states of Bavaria and North Rhine–Westphalia is also the same as in Baden-Württemberg. For all other European countries, there exist no such numbers unfortunately. It has been reported, however, that there is not a single person with technical expertise working for the Austrian DPA, for example.

Since May 2018, the number of complaints by data subjects has increased considerably in Baden-Württemberg, from nearly 200 in the beginning of 2018 to roughly 4,000 after the 2018 enforcement date of the GDPR. In contrast, the number of complaints in 2017 and 2016 was approximately 3,000 and 2,000, respectively. The number of data breach notifications has also been at a consistently high level since May 2018, with an average of roughly 100 data breaches reported to the BW-DPA each month. When looking at other European countries, a similar picture emerges: the European Data Protection Board published numerous figures on its website of European DPAs one year after GDPR enforcement began. According to the report, 144,000 queries and complaints and 89,000 data breach notifications were retrieved by DPAs within one year.

Relevant Articles Regarding Technical Aspects in the GDPR

Technical Obligations for Controllers

This section details those articles of the GDPR that have a close relationship to technical aspects. Regarding technical data protection in particular, Articles 25 and 32 address the obligations for controllers.

Article 25, "Data Protection by Design and by Default," obligates controllers "… both at the time of the determination of the means for processing and at the time of the processing itself" to "implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation." Moreover, the controller "shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."

Article 32, "Security of Processing," requires that "the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk." It is explicitly mentioned that the ongoing confidentiality, integrity, availability, and resilience of processing systems and services need to be ensured. In addition, it is required that the effectiveness of technical and organizational measures for ensuring the security of the processing is regularly tested, assessed, and evaluated.

Another relevant article with regard to technical data protection is Article 33, "Notification of a Personal Data Breach to the Supervisory Authority," obligating the controller to notify the supervisory authority of a personal data breach no later than 72 h after having become aware of it (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons).

Article 35, "Data Protection Impact Assessment," requiring the execution of a data protection impact assessment (DPIA) in cases where a type of processing "in particular using new

technologies" is "likely to result in a high risk to the rights and freedoms of natural persons," is also seen as a requirement residing more in the technical area by most lawyers.

Rights of Data Subjects

The (new) data subject rights introduced in the GDPR are also interesting from a technical point of view. First, Article 15, "Right of Access by the Data Subject," provides the data subject the right to obtain from the controller "confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data." Access to personal data means that the controller "shall provide a copy of the personal data undergoing processing." What makes this article interesting from a technical point of view is that the information shall be provided in a commonly used electronic form "if the data subject makes the request by electronic means." Another important article is Article 17, "Right to Erasure ('Right to Be Forgotten')." It states that the "data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" (if the personal data are no longer necessary, the data subject withdraws consent on which the processing is based and so on). Furthermore, if the controller has made the personal data public, it shall take "reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested to erasure by such controllers of any links to, or copy or replication of, those personal data." Finally, there is Article 20, "Right to Data Portability," which is a new right introduced to privacy law following the enactment of the GDPR. According to this article, the "data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided." At the same time, this right "shall not adversely affect the rights and freedoms of others."

Challenges and Open Questions

From the professional (daily) practice of handling data subjects' complaints and dealing with inquiries and data breach notifications by companies (among others), a number of challenges and open questions have been determined regarding the proper implementation of the GDPR's technical requirements.

Who Is Responsible? Who Can Do It? State of the What?

One of the most obvious problems concerns the demand for PbD and privacy by default (Article 25). The demand explicitly addresses the controller, and not the developer. This means that DPAs can only prosecute controllers who use software that is not designed according to PbD principles and, thus, is able only to have an impact on the developer in the long run if enough controllers demand software designed according to PbD principles. This, however, has not yet happened. The situation is especially problematic in cases where only few developers dominate the market. A widespread operating system, for example, is known for its (by default) transfer of (personal) data to its developer. The operating system is available in different versions. Only the most expensive version (targeting big enterprises) allows for the full deactivation of transfers (and, thus, is the only version currently accepted by DPAs). Yet

this version is not affordable for small companies or social clubs. It would most likely not be accepted if DPAs were to prosecute such small companies or social clubs, even if they violate Article 25 by using the (wrong version of the) system. The same holds true for other software.

The European Union Agency for Network and Information Security (ENISA) published "Privacy and Data Protection by Design" in 2015. This report, which aims to close the gap between legal requirements and available technology, is often referred to by researchers, mostly (but DPAs and companies also refer to the report). Among the privacy-enhancing technologies mentioned are "attribute-based credentials," "private information retrieval," "searchable encryption," "homomorphic encryption," "oblivious transfer," "differential privacy," and so on. With the exception of differential privacy, which has recently found its way into practice, none of these technologies can truly be seen as state of the art; rather, they are deemed "state of research." Consideration for the state of research has been demanded by the European Parliament during the GDPR's legislative procedure, but it has not explicitly been considered for inclusion in the GDPR. Thus, developers do not really know which technology qualifies as an implementation of the PbD requirement. Most DPAs will not be able to fulfill the requirement of the ENISA report, which requires DPAs to assess privacy-enhancing technologies and consult with companies on which technology to use; rather, the report would require computer scientists with a strong background in technical privacy protection to do that.

A good example for the misinterpretation of PbD is the 2016 German Federal Law "Digitisation of the Energy Transition," which concerns domestic equipment and the operation of smart meters. The term PbD can be found four times in the law; for instance, a "privacy-by-design standard" of the German Federal Office for Information Security shall guarantee PbD. On the other hand, PbD in this "standard" means only "standard" encryption of transmitted electricity consumption data. This is especially remarkable when one considers that research on privacy-friendly smart metering has been actively pursued by researchers worldwide since roughly 2009; a Google Scholar search reveals thousands and thousands of research papers on privacy-friendly smart metering. Yet none of those considerations has been used in practice.

Email Encryption: A Never-Ending Story

Regarding Article 32, the same challenge exists as previously mentioned in the discussion of Article 25: in general, it is not easy to determine which security measures are state of the art. A good example is the case of email encryption, which has been intensively discussed among DPAs for years (or even decades) and is again current as of May 2018. The question is whether controllers can be forced to provide the opportunity for end-to-end (E2E) mail encryption (based on Pretty Good Privacy or Secure/Multipurpose Internet Mail Extensions), so that natural persons are able to securely communicate with them. Although the technology has been available since the early 1990s, few people use it. Can E2E-mail encryption therefore be regarded as state of the art? Perhaps it would be more advantageous to look for alternative solutions that provide similar security but with a much lower barrier to usage for most users. Instant messaging (where E2E encryption and perfect forward secrecy are standard today) could be such an alternative, yet the most popular instant messaging service is viewed skeptically by DPAs due to its transfer of contact details to the provider for the purpose of contact matching, for which no practical privacy-friendly solution currently exists.

Another interesting point is that, as stated in Article 32, one can gather penetration testing as a requirement. Although it would also have been a good idea to perform penetration tests in the past, this requirement had not previously been explicitly stated in German privacy law.

Does Security Improvement Raise the DPA's Attention?

Continuing with the need for penetration tests, there is another challenge regarding Article 33. Whenever "solid" penetration tests are conducted (by independent parties) in practice, some security issues are uncovered. If a vulnerability is found, the concern for the controller is whether the DPA needs to be notified about it. A vulnerability that allows external parties to (potentially) access a large number of sensitive personal data (e.g., special categories of personal data, according to Article 9) could result in a risk to the rights and freedoms of natural persons and, thus, would need to be seen as a "personal data breach." According to Article 33, this outcome is notifiable, even though the vulnerability is most likely not found and abused by attackers (because it is fixed shortly after discovery). A controller who is especially exemplary in conducting penetration tests on a regular basis to guarantee the best security could feel being punished for his or her efforts because he or she will need to notify the DPA more often. This may raise the DPA's suspicions about the controller, which is not the controller's intention. A controller who does not perform solid penetration tests on a regular basis, on the other hand, will not run into this "problem." Regarding the aforementioned example in this section, it is even imaginable that a high risk for natural persons could be assumed, and, thus, the controller would need to notify the data subjects, according to Article 34. The question for many controllers is whether they can use information from log files as proof that nobody exploited the system's vulnerability and accessed the data, thereby eliminating the need for notifying data subjects. In general, this question is not easy to answer; rather, it is a case-by-case decision made, in part, as a result of the discussion between the controller and DPA after notification, according to Article 33.

Since 2018, it has been discovered that controllers report (supposed) data breaches too often, typically out of fear of a fine being imposed for not notifying the DPA (if the DPA took note of the event and qualified it as a data breach). Consequently, for example, DPAs receive a large number of data breach notifications for cases where someone sent an email to the wrong recipient.

Interplay Between Engineers and Lawyers?

Performing a solid DPIA according to Article 35 is a challenging task that requires the person conducting it to have in-depth knowledge. If one thinks of processing "using new technologies" (Article 35, para. 1), for example, the use of artificial intelligence, it would require an understanding of the used technology to perform a valid assessment of potential risks to the rights and freedoms of data subjects. On the other hand, DPIAs are often conducted by data protection officers, who do not typically have the knowledge of such technology and are thus not able to conduct a thorough analysis. This might be the reason that a single solid DPIA has not yet been received by the BW-DPA. Unfortunately, most DPIAs are nothing more than a list of technical and organizational measures, according to Article 32. Cooperation among people with both technical and legal expertise would be essential for conducting a thorough DPIA.

Data Subject Rights as Boomerangs?

Thus far, obligations for controllers have been discussed. The rights of data subjects are now examined. Article 15 is a fundamental right of data subjects, allowing them to obtain from the controller information not only about (among other things) which personal data are being processed and the purpose, but also to obtain a "copy of the personal data undergoing processing" (Article 15, para. 3). As previously stated, information shall be provided electronically if the data subject makes the request using electronic means. Legislators wanted to ease the retrieval of information for data subjects from controllers: a request that is permitted to be made via email lowers the hurdle for data subjects to make use of their rights, but email is not the best communication medium for that purpose. First, an email (without a digital signature) does not provide any form of authentication. The sender of an email can be easily forged, which throws the doors wide open for faked requests. It would be easily possible for somebody to pretend to be somebody else and request the personal data from the controller of the spoofed data subject; with knowledge about the target person, it would be easy to respond to security questions by the controller, if there are any (e.g., date of birth, place of residence, etc.). Thus, the well-meant strengthening of rights of data subjects could easily turn out as a boomerang for them.

Requesting the presentation of (a digital copy of) an identity document, which is often done in practice, is not a secure identification method either, as fake copies can easily be produced. Moreover, presenting only an identity document does not protect against fake requests from people who are able to obtain an identity document of the target person (e.g., roommates or family members). For instance, a wife could make use of Article 15 to find out whether her husband is using a dating platform (and even acquire further information from the dating platform). Unfortunately, it will only be a matter of time before fraud occurs in that regard. It should be noted that the problem of identification is not only prevalent with Article 15; it should also be taken into account regarding Article 16 ("Right to Rectification"), Article 17, Article 18 ("Right to Restriction of Processing"), and Article 20. More secure identification methods exist and their use is imagined for that purpose [e.g., electronic identification based on the electronic IDentification, Authentication and trust Services (eIDAS) Regulation, video chat identification, and so on]. Better security, however, means more expenditures for controllers and data subjects. It will be interesting to see whether data subjects will accept strong identification procedures (which should be in their own best interest).

Another aspect of responses to Article 15 requests via email is that email does not provide confidentiality. Thus, sensitive personal data, which can be a part of Article 15 responses, should not be transmitted unencrypted, but in practice, E2E mail encryption is generally not used by data subjects.

Availability/Integrity Versus Right to Erasure?

Article 17, another fundamental right of data subjects, is especially challenging in connection with Article 32. According to Article 32, the controller must have "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident." This can only be achieved by means of a backup. Yet what happens if a data subject, whose personal data are present not only in the current system but also in the

backup, makes use of his or her right to erasure? Does the controller also need to delete the personal data of the data subject from the backup? From a technical perspective, deleting individual data from a backup is—if even possible—highly problematic. The integrity of a backup is fundamental, but lawyers insist that personal data also must be deleted from the backup, because there is no exception provided in the GDPR for data that are backed up. In this case, the organizational methods that prevent access to data in the backup are not sufficient for lawyers. Erasure means that the data must be deleted everywhere. It will be interesting to see (also with regard to Article 25) whether backup software providers will provide solutions for that task.

Data Portability: Still Unknown or Not Needed?

According to Article 20, "data portability," introduced with the GDPR, is a new right for data subjects. It should provide data subjects with the possibility to escape lock-ins with service providers. Note that not a single request concerning data portability (neither by data subjects nor by controllers) has been received within a year by the BW-DPA, and thus far, this topic appears to be irrelevant for most data subjects and controllers. Data portability in social networks, which certainly was a major scenario for legislators, additionally introduces some interesting challenges. As the rights of others shall not be affected, friendship relationships cannot be ported from one social network to another that easily, because a friend in one social network might not want the relationship with a user making use of his or her right to data portability to be mapped in another social network as well. Thus, only personal data without any reference to others' personal data are "portable," which, in the end, decreases the potential benefit of data portability. Additionally, if the right for data portability is interpreted strictly, only outgoing (and no incoming) messages on a communication platform would be ported, for example, because only outgoing messages were provided to the controller by the data subject him or herself. This would further decrease the benefit of data portability.

Conclusion and Outlook:
Technical data protection does not (yet) play the role that it was presumed to play beforehand, based on experiences during the first year of GDPR application. Companies and authorities do not yet have the necessary expertise to properly implement technical data protection. In times of skills shortages, this is not expected to change in the (near) future. Unfortunately, the same holds true for DPAs. DPAs do not appear to be attractive employers for well-educated computer scientists. Comparing the numbers previously discussed (that is, the sole person with a technical background being responsible for 100,000 companies), one can easily see that comprehensive enforcement is difficult to achieve on a grand scale. The investigation of a single ("real") data breach is a cumbersome task that must be adequately thorough to withstand a court proceeding.

In 2017 and 2018, a number of companies spent a considerable amount of money for law firms to be GDPR compliant; however, a small portion of that money appears to have been spent on technical data protection and information security. To a great extent, the challenges discussed in this article are due to a lack of technical knowledge in legislation. This shortcoming can be found in a number of laws concerning technology, and, unfortunately, in the GDPR as well. For controllers and DPAs, this problem does not ease application of the GDPR.

In some (important) areas, we are still at the beginning, even after one year of GDPR enactment. The GDPR envisages privacy certifications, for example, but not a single certification authority has been accredited by DPAs in Germany after one year. Thus, companies could not yet obtain certifications for their products.

This article has mentioned the problem that Article 25 addresses developers, but it does not obligate them, which contradicts the idea of PbD. What we see, in practice, is that developers are not "encouraged" to provide privacy-friendly products by default (as envisaged in Recital 78, section 4). This is why we will suggest that the European Commission, as part of the evaluation of the GDPR (Article 97, Sections 1 and 3), should obligate developers to meet the requirements; the obligation is comparable to what Council Directive 85/374/ EEC states with regard to liability for defective products.

On a positive note, the first fines for violations of the GDPR in Germany were due to a lack of implementation of technical and organizational measures, which were issued by the BW-DPA. Today, more than one-half of all fines issued in Baden-Württemberg were due to violations of requirements for technical data protection, which totaled €250,000. This is especially noteworthy because such violations were not previously fined in Germany. Other DPAs, such as the Information Commissioner's Office in the United Kingdom, go even further with their (notices of intention for) high fines against Marriott and British Airways, which were also due to a lack of technical data protection.

Moreover, it has been noticed that project management agencies in Germany now request (potentially "problematic") directors of to-be-funded projects to consult with the DPA beforehand to clarify whether the project is at all compatible with the GDPR and that DPA suggestions be implemented during project execution. This provides a great opportunity for experts to participate in research projects and introduce their expertise in implementing technical privacy protection.

Author information:
Ronald Petrlic is a professor of information security at TH Nürnberg. Prior to that, he was the head of the technical department of the Data Protection Authority in Baden-Württemberg, Germany. His research interests are the General Data Protection Regulation, technical privacy protection, and information security. Petrlic received a Ph.D. in computer science from Paderborn University, Germany. He authored the first German textbook on privacy by design. Contact him at ronald.petrlic@th-nuernberg.de.