Brussels Calling: Big Data and Privacy

Nicolai Culik

Abstract The planned General Data Protection Regulation (GDPR) will fundamentally reform the data protection law in Europe. In Germany, the GDPR is going to replace the current Federal Data Protection Act (Bundesdatenschutzgesetz) and will be directly applied by the authorities and courts. The GDPR has been negotiated since 2012 by the European Commission, Council and Parliament. It will enter into force in May 2018. The different levels of data protection within the EU are supposed to be standardized. There will be some areas, however, in which the member states will be authorized to enact own laws (e.g. regarding employee data protection). This paves the way for the further development of big data. The GDPR will—as far as foreseeable—loosen the screws on some relevant focal points of the data protection law, such as the principle of purpose limitation. However, this will not go as far as critics have feared. The German data protection level will be slightly lowered, while the European level will be raised on average. This will also have a positive impact on German actors at times of cloud computing and cross-border data processing.

1 Data Protection on the EU-Level

> If the purpose of this reform was to strengthen people's control over their personal information and improve enforcement, our governments have achieved the exact opposite.
>
> Anna Fielder, Privacy International

Data protection is no longer a national topic. Due to the digitally closely linked, increasingly merging global village the EU has been authorized by its member states to set the course in this area as well.[1] Initially, this constituted broad

[1]Since the Treaty of Lisbon (2009), the relevant competence basis for the area of data protection is Art. 16 para. 2 TFEU.

N. Culik (✉)
Institute for Information, Telecommunication and Media Law (ITM),
University of Münster, Münster, Germany
e-mail: nicolai.culik@uni-muenster.de

T. Hoeren and B. Kolany-Raiser (eds.), *Big Data in Context*,
SpringerBriefs in Law, https://doi.org/10.1007/978-3-319-62461-7_4

sector-specific targets. In order to regulate data protection comprehensively, the European Parliament subsequently adopted the Data Protection Directive. This directive has been implemented in national law by the individual member states within the limits of the scope granted to them.[2] Thus, no full but at least a minimum harmonization could be reached. It is problematic though, that the Data Protection Directive dates back to the year 1995, a time when by no means every household had a computer, let alone internet access. One could not speak of smartphones since hardly anyone even owned a cellphone back then. Describing the Internet as "new ground"[3] would have been appropriate at that time.

In short: The EU-Directive, on which the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) is based, is no longer up to date. Additionally, the different implementation in the 28 member states has led to an uneven data protection level within the EU. Besides low taxes, this is also one reason why Facebook has its European headquarters in Ireland, a member state with comparatively liberal data protection.

Now, everything shall be changed. The passed General Data Protection Regulation (GDPR) shall ensure a full harmonization in the area of data protection law. Insofar, the title "General Regulation" has a legal as well as a symbolic meaning: The difference from a legal perspective is that regulations have direct effect. As opposed to directives, they do not require transposition into national legislation.[4] Symbolic is the name "General" Regulation: On the one hand, it is supposed to emphasize the aspiration to regulate the topic of data protection comprehensively. On the other hand, member states shall be granted a scope for detailed national rules.

2 Genesis of the General Data Protection Regulation

The serve for the GDPR was made by the European Commission under the leadership of the former Luxembourgish Justice Commissioner Viviane Reding at the beginning of 2012. Subsequently, the LIBE Committee[5] submitted a compromise version to the Parliament, for which more than 3.000 amendments were proposed while only 207 were eventually included in the draft. In summer 2015, the Council, which consists of the minister of the member states, agreed on a common position as well.

Therefore, the way was clear for the negotiations between the three institutions, which are prescribed by the EU Treaties and currently ongoing. However, they did

[2] See Art. 288 para. 3 TFEU.

[3] Said *Angela Merkel* on 19 Jun 2013 during a press conference on the occasion of the visit of US-President Barack Obama.

[4] See Art. 288 para. 2 TFEU.

[5] From the English name: *Committee on Civil Liberties, Justice and Home Affairs*.

not take place—as so often—according to the officially provided procedure[6] but as a so-called "*informal trialogue*" behind closed doors. On the one hand, this approach draws criticism regarding the lack of transparency of the EU's work, which has been pilloried for its democratic deficit anyway,[7] and the strong influence of various lobby groups. On the other hand, the hope was fueled to quickly achieve a result after a time of tough negotiations. A conclusion of the negotiations was achieved by the end of 2015. A timely adoption surely had a signal effect, especially regarding the transatlantic data protection debate with the USA which has gained additional significance after the Safe Harbor judgment by the ECJ[8] on October 6, 2015. The GDPR was officially passed in May 2016; it will be applicable two years later.

3 General Criticism of the General Data Protection Regulation

The GDPR is mainly criticized for two issues: Firstly, the General Regulation is said to come closer to a directive in its effect. This argument is based on the numerous opening clauses, thus on the passages in which only broad provisions are given, leaving the exact modalities to the member states. An example for this is the area of employee data protection: The GDPR provides in Art. 88 that "*Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context*". In Germany, there was even a draft law for an Employee Data Protection Act (Beschäftigtendatenschutzgesetz). The initiative was put on ice, however, in order to wait for the Regulation. It is already being debated what is exactly meant by "*more specific rules*". Due to this room for interpretation, different rules in the member states can be expected, which was actually meant to be prevented.

Secondly, it is feared that a deficit of legal protection of the citizen could arise. EU law takes precedence over national law. Particularly, the scope of the Regulation affects fundamental rights as well, such as the right to informational self-determination. If a citizen feels that his rights have been infringed, no longer the Federal Constitutional Court (Bundesverfassungsgericht) in Karlsruhe but the ECJ in Luxembourg has jurisdiction. Yet, on the European level, there is no constitutional complaint. In a case coming down to the validity of the Regulation, the citizen would depend on a national court referring the matter to the ECJ.[9] It is not

[6]This is specified in Art. 294 TFEU.

[7]See the protest letter which was published among others by EDRI on 30 Sep 2015.

[8]Regarding this topic see chapter "Safe Harbor: The Decision of the European Court of Justice", p 41 et seqq.

[9]So called preliminary ruling procedure under Art. 267 TFEU.

uncommon that in practice German judges shy away from this procedure, probably also because European Law has not yet played a big role during their own legal training finding themselves on rather shaky ground. Whether this deficit of legal protection actually arises, remains to be seen.

4 Possible Consequences for Big Data

The consequences of the new law for big data innovations can be determined based on a short analysis of the principle of purpose limitation, which is one of the most important German and European data protection principles. This certainly "sharpest sword" of data protection is opposed to the unlimited linkage of large amounts of data.[10]

The principle of purpose limitation states that personal data may only be collected for a precisely specified, clear and lawful purpose and that it cannot later be processed for a purpose incompatible with these provisions.[11] The data producer therefore has to inform the affected person about the purpose when collecting the data and has to comply with this purpose during the processing. Many big data applications, however, are precisely based on linking data that has been collected from different sources, at different times, in different contexts and for different purposes.[12] Often, data is simply collected to consider later on what it could be useful for as well. The principle of purpose limitation yet requires that the person responsible for the data collection or processing considers the data use or business model in advance. This requirement thus contradicts big data.

What rules concerning this important principle are provided in the GDPR? Can the accusation by *Privacy International* cited above be justified?

According to the Council's proposal, "*further processing of personal data for (…) scientific, statistical or historical purposes shall (…) not be considered incompatible with the initial purposes.*"[13] The question arises what exactly is meant by these terms, since they are not further defined in the proposal. This also begs the question whether the data analysis through big data analysis tools is not always for statistical purposes.

Furthermore, the Council, of which among others Federal Minister of Justice *Heiko Maas* (SPD) is a member, wanted to add a further exception to the principle of purpose limitation: "*Further processing by the (…) controller or a third party shall be lawful if these interests override the interests of the data subject.*"[14] In this

[10]Weichert, ZD 2013, p 252.

[11]See Art. 5 para. 1 lit. b GDPR.

[12]Kring 2015, Big Data und der Grundsatz der Zweckbindung. http://subs.emis.de/LNI/Proceedings/Proceedings232/551.pdf.

[13]See Art. 5 lit. para. 1 lit b GDPR Council draft.

[14]See Art. 6 para. 4 GDPR Council draft.

regard, it should be noted that a legally imposed balancing of interests always entails a certain degree of legal uncertainty. The same applies to the purpose of the data processing. It is not yet clarified how precise and on which level of abstraction the term “purpose” has to be defined.[15] According to the legislative proposal, the interests of third parties, such as the economic interests of companies offering big data analysis, could possibly be invoked. It should be noted that the choice of terminology in the draft was very imprecise. That this softening of data protection principles was surely desired by the German negotiating side is proven by the statements made by Chancellor *Angela Merkel* at the IT Summit 2015.[16]

The approved GDPR clarifies that the outcome of data processing for statistical purposes must not contain personal data or be used for measures against natural entities.[17] Consequently, many big data applications are not affected by the exception of the principle of purpose limitation.

The balancing of the interests was also not included in the final version of the GDPR. Originally, the council wanted to use this balancing to allow changes of purpose.

However, there are now certain criteria that must be respected by the data processor regarding the question, whether the new purpose is still compatible with the original one. The possible consequences of the intended processing for the data subject are one example for these criteria, Article 6 para 4 lit. d GDPR.

The remaining criteria are ill defined as well and therefore cause different national interpretations.[18] Ultimately, there still has to be a weighing of interests. The explicit naming of this phrasing was given up on the basis of heavy criticism, but the already mentioned compatibility of the new purpose with the purpose of the collection means exactly the same.

Only an extensive jurisdiction is able to react to these uncertainties. The regulation has direct effect and therefore cannot be differentiated by the national legislators.

5 Conclusion and Outlook

Against this background, the statement by Anna Fielder cited above cannot totally be objected: The Analyzation of the principle of purpose limitation has shown, that people’s control over their personal data and enforcement in this context did not improve, compared to the data protection directive that still is in force. Although, if European governments have actually achieved “the exact opposite” might be an

[15]Dammann, ZD 2016, p 312.

[16]See the statement by *Angela Merkel* from 20 Nov 2015.

[17]Recital 162 GDPR; see Buchner/Tinnefeld 2016, in: Kühling/Buchner (eds), DS-GVO Kommentar, Art. 89 Ref. 15.

[18]Roßnagel et al. 2016, Datenschutz 2016—Smart genug für die Zukunft? p 158.

exaggerated statement. It must be examined in the near future, how the numerous opening clauses are going to be filled out by the member states. Especially for German standards, the GDPR does not involve a significant change regarding the central purpose limitation principle. In German law, there also are exceptions for a change of purpose. These exceptions are in fact a bit more restrictive, but quite comparable.

However, data protection can no longer be thought of only within national borders which is proven for example by the practice of cloud computing. In many other European countries, such as Ireland or Romania, the protection level will rise.[19] Thus, the standardization will eventually still have a positive effect on affected parties in Germany.

References

Beuth P (2013) Die Kanzlerin von Neuland Die Zeit. http://www.zeit.de/digital/internet/2013-06/merkel-das-internet-ist-fuer-uns-alle-neuland. Accessed 4 Apr 2017

Buchner B, Tinnefeld M (2016) In: Kühling J, Buchner B (eds) DS-GVO Kommentar. C. H. Beck Munich. Art. 89 Ref. 15

Coalition of 33 Civil Rights Organizations (2015) Letter. https://edri.org/files/Transparency_LetterTrialogues_20150930.pdf. Accessed 4 Apr 2017

Dammann U (2016) Erfolge und Defizite der EU-Datenschutzgrundversorgung. ZD 6(7):307–314

Krempl S (2015) Merkel auf dem IT-Gipfel. Heise Online. https://www.heise.de/newsticker/meldung/Merkel-auf-dem-IT-Gipfel-Datenschutz-darf-Big-Data-nicht-verhindern-2980126.html. Accessed 4 Apr 2017

Kring M (2015) Big data und der Grundsatz der Zweckbindung. http://subs.emis.de/LNI/Proceedings/Proceedings232/551.pdf. Accessed 4 Apr 2017

Roßnagel A et al. (2016) Datenschutz 2016—Smart genug für die Zukunft? http://www.uni-kassel.de/upress/online/OpenAccess/978-3-7376-0154-2. OpenAccess.pdf. Accessed 4 Apr 2017

Weichert T (2013) Big Data und Datenschutz. ZD 3(6):251–259

Author Biography

Nicolai Culik Dipl.-Jur., research associate at the Institute for Information, Telecommunication and Media Law (ITM) at the University of Münster. He studied law in Constance, Lyon and Münster, from where he holds a law degree.

[19] The appointment of a data protection officer, for example, has not so far been obligatory in many countries but will be introduced by Art. 35 GDPR.