Specifying the GDPR: Member States perspectives Series: Germany

Summary prepared by Michalina Nadolna Peeters[1]

On 12 November 2020, the Brussels Privacy Hub (BPH) organised the second event of the series "Specifying the GDPR: Member States perspectives" ("Series") which aims at providing an overview of national perspectives and legal developments related to the General Data Protection Regulation (GDPR).

The event was devoted to the developments in **Germany**. The speakers were **Orla Lynskey** (Associate Professor of Law at London School of Economics, General rapporteur on Data Protection at the FIDE 2020 Congress) and **Andreas Wiebe** (Professor at Georg-August-University of Göttingen).

The conversation was chaired by **Gloria González Fuster** (Research Professor at VUB), who opened the discussion by presenting the Series and the speakers.

Orla Lynskey presented the key finding from the Report entitled "The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection" prepared for the XXIX International Federation for European Law (FIDE) Congress in the Hague taking place in May 2021. Orla Lynskey explained that apart from the mentioned report, there are also two other ones – "National Courts and the Enforcement of EU Law – the pivotal role of national courts in the EU legal order" and "EU Competition Law and the Digital Economy – protecting free and fair competition in an age of technological (r)evolution)".

Orla Lynskey noted that the EU Law Live Podcast Series has recently released a podcast featuring herself, Anna Buchta and Herke Kranenborg - available here.

For each report, a general rapporteur is chosen. For the report concerning data protection, the general rapporteur was Orla Lynskey. She prepared the questionnaire shared with FIDE Members in EU Member states, Norway and Switzerland. She focused on the aspects of the GDPR where she expected to see the most development, divergences or common problems emerging at national level.

The questionnaire was meant to address both broader EU law questions, such as the impact of the Charter of Fundamental Rights of the EU on data protection law, as well as specific EU data protection questions. It is divided in four parts: 1) setting the scene, 2) the reception of substantive provisions in the national legal order, 3) domestic

[1] PhD Researcher BPH-LSTS/ VUB.

enforcement of data protection law, and 4) data processing for national security purposes.

The Report is a combination of General, Institutional and National reports. In her capacity as the general rapporteur, Orla Lynskey compared and evaluated the findings from the national reports in her General Report, which is accompanied by the Institutional Report authored by Anna Buchta and Herke Kranenborg.

Orla Lynskey first addressed the topic of flexibilities provided by the GDPR to Member States and differences in availing of them. She noted that the GDPR, despite being a regulation, gives a very broad scope of leeway for national variations. This leeway was used by some Member States in a far-reaching manner, while other Member States were more reserved in their use of such possibilities. In this context, Orla Lynskey highlighted the distinctive aims of Member States when receiving the GDPR into national laws. Finland's main purpose was to ensure the preservation of the status quo and have the least disruption between the Data Protection Directive (DPD) and the GDPR. Austria and the Czech Republic, on the other hand, sought to prevent gold-plating of data protection standards (going beyond the standards provided for in GDPR) to make sure the burden on SMEs is minimal.

Orla Lynskey paid particular attention to the differences in the implementation of Art. 5 GDPR (principles relating to processing of personal data). She noted that so far there has been very little guidance on the principle of fairness, and the principle of purpose limitation. She found that in some Member States, like Slovenia, the principle of fairness has been often used. However, divergence between Member States was considerable. Some equate fairness with transparency, others – with good faith, due diligence, protection against discrimination, or something that correlates to the reasonable expectation of data subjects. Also, consent and legitimate interest can be differently understood across Member States. In some there is a failure to recognise that the GDPR places all Art. 6 GDPR bases on equal footing because of national constitutional protection surrounding consent.

As another example, Orla Lynskey provided Art. 23 GDPR which allows for some limitations to specific rights. In France, the right to information is limited where data is indirectly collected for taxation purposes. In the Czech Republic, Art. 23 GDPR was interpreted in such a way that limitations are possible without further legislative acts as long as they are notified to the National Supervisory Authority (NSA). She noted that the Czech report states that it seems impossible to comprehensively list all of the possible restrictions.

In addition, several reports noted that the result of the GDPR is a very complicated legal system at national level, as some national instruments incorporate the GDPR while also implementing the Law Enforcement Directive (LED) and national security provisions.

The second aspect discussed by Orla Lynskey was the composition and enforcement record of NSAs. In terms of the composition, she noted that most NSAs comprised of a President or Commissioner, but that some did not follow this structure, e.g., the French NSA has a multidisciplinary college with political appointees. She also noted that NSAs have various forms of expert groups providing non-binding advice to them. In addition, she concluded that the staffing levels vary drastically across the countries, with most having between 30 and 80 members of staffer. Here, an important outlier is the UK which has somewhere around 700 members of staff.

With regard to the enforcement records, Orla Lynskey noted that on national level it is difficult to track the cases because there are no coherent reporting systems. In some cases, reports mentioned statistics on complaints introduced, in some others reports reference was made to the number of procedures launched. Nevertheless, she stated that there a consistent increase in demand for NSA action since the entry of the GDPR into force.

Further, Orla Lynskey discussed strategic enforcement. The main purpose of this was to assess to what extent NSAs pursue a selective approach to their enforcement or engage in another type of triage mechanism. She noted that very few NSAs are required by law to pursue all complaints (exceptions are e.g., Malta and Portugal). In addition, in some Member States there are procedural impediments or requirements before a complaint can be brought to an NSA (e.g., Greece – submit a prior complaint to a controller or Data Protection Officer (DPO) before submitting complaint to NSA). In other Member States, there is some sort of explicit or implicit selective enforcement. In these cases, the NSAs follow up with complaints that they perceive to be the most important for a number of reasons. For instance, in the UK enforcement can be intelligence-led.

The last area discussed by Orla Lynskey was private and collective enforcement under the GDPR. She noted that there is consistent acceptance that an infringement of data protection could lead to non-material harm. A notable exception is the UK and Ireland, where damages for non-tangible harm was initially contested. Nevertheless, there are differences in how damages are recognised. In some Member States, it is presumed that the violation leads to a harm. However, in others separate evidence of harm needs to be provided. Still, when damages are awarded, courts have difficulties in quantifying harm where it is nonmaterial. The amount of damages is often symbolic.

With regard to collective enforcement, Orla Lynskey noted that there has been a very low take up of Art. 80 GDPR to allow for representative action in Member States. It seems that only France has availed of the full possibilities offered by Article 80. When it comes to Art. 80(1) GDPR, there is still a number of restrictions to the notion of qualified entity. In some States, for instance, there is a requirement that such entities have been established in a Member State for more than 5 years. She noted that there are Member States where there are no qualified entities, e.g., Slovenia.

As a final remark, Orla Lynskey pointed out that despite the Europeanisation potentially brought about by the creation of the European Data Protection Board, we will see a lot of differentiation at the national level.

Andreas Wiebe focused on the case of Germany in his presentation. He reminded that Germany is a federal state, which means that there are 16 state laws on top of federal law, and that there are 17 state data protection commissioners and 1 federal commissioner. This means that the German legal landscape is diverse on both horizontal and vertical level. As such, there was a difficulty in implementing the GDPR into law, and that the completely redrafted GDPR entered in force in 2018. He noted that it kept the classical separation between public and private sector which is not excluded by the GDPR and does not have effect on the substance. That approach already is, however, a point of discussion regarding correctness of transposition.

Andreas Wiebe noted that the German legislature made use of several opening clauses provided for in the GDPR. For instance, Art. 9(2)(g) and (h) GDPR was implemented in §22 BDSG (German Federal Data Protection Act) to allow for the processing of health data, esp. sensitive data. Still, there is a high demand for refurbishing the data processing rules in the health sector. Another example is Art. 23 GDPR. Andreas Wiebe pointed out that German legislator introduced several deviating norms in §§32-37 BDSG that more or less keep up a sound level of protection. An example would be §32 which provides an exception to the right to inform the data subject in cases of change of purpose pursuant to Art. 13(3) GDPR.

On top of these, there are sector specific amendments contained in 154 special statutes, which adapt the wording, legal grounds and data subjects' rights. For instance, the minimum number of employees to requiring a DPO, previously already based on an opening clause, was raised from 10 to 20 in order to alleviate the burden for SMEs. In employment, consent was extended to written and electronic form (§26 Abs.2 Satz 3).

Further, Andreas Wiebe proved additional specificities of the GDPR transposition in Germany. For instance, §31 BDSG stipulates some requirements for the use of scoring, although there is no basis in the GDPR. §34 BDSG makes use of Art. 23 GDPR possibility to limit some rights, specifically it limits the right to be informed in some cases. In this context, he noted that §34 BDSG may potentially clash with Art. 10 of the Bavarian Data Protection Act (BayLDSG) because it is differently structured and differs in detail. §34 BDSG mentions public security and "disadvantages for the welfare of the Federation or a State", whereas the Bavarian rule mentions "an important economic or financial interest of the State of Bavaria , another State, the Federation or the EU", explicitly citing "Currency, budget and tax affairs".

Further, Andreas Wiebe mentioned the existence of the links between competition law and data protection law, especially in the context of the market dominant position. For instance, the German Competition Authority prohibited Facebook from merging user data from different sources (WhatsApp and Instagram) finding that collection of personal data in social network may constitute abuse of dominant position in two-sided markets.

Andreas Wiebe also discussed the importance of the e-Privacy Directive. A recurring issue has been the status of the data protection rules of the telecommunications law - Telemediengesetz (TMG). The prevailing view was that §§12-15 TMG are not applicable anymore because have been pre-empted by the GDPR. However, Germany had not properly implemented Art. 5(3)(e) e-Privacy Directive despite the government claiming to have done so. After Planet49 judgment of the Court of Justice of the European Union (CJEU), there was a follow up judgement (BGH 28.05.2020, Az.: I ZR 7/16) where the German court stated that §15 TMG is still applicable and is to be treated as an implementation of the GDPR. As such, consent has to be clear which products and services are included, and that it is not sufficient to point to a long list of partners to deter him from the choice.

Andreas Wiebe further discussed an interesting development concerning enforcement through collective action under the German Act against Unfair competition (UWG). This act contains specific collective enforcement mechanisms in unfair competition law. §3a provides for a special rule that breach of a market oriented legal provision amounts to unfair competition. Even before the GDPR it was debatable if and to what extent data protection provisions could constitute relevant market related provisions. Now, it is also widely discussed whether UWG may be used as an instrument of enforcement of the GDPR. There is a fear, however, that this instrument would be used by associations and law firms specialised on warnings on a large sale to sue big and small companies for breach of data protection law. Andreas Wiebe pointed out that the central question in this dispute is whether the GDPR provides for a full sanction system that precludes any legal action under the UWG. Commentators as well as courts are split on this issue and there is conflicting caselaw on the matter. In the FashionID judgment, the CJEU decided that Arts. 22-24 of the DPD do not preclude national rules to give a standing to associations. However, it is not clear how this would be evaluated under the GDPR which is a regulation. In June 2020, a preliminary question was brought to the CJEU to ask whether the GDPR precludes additional enforcement grounds provided for by the UWG.

Andreas Wiebe also noted that there has been a political agreement reached with regard to Directive on the protection of collective consumer interests, which would allow for collective action also in case of GDPR infringements and thus turn the tide towards collective actions.

Andreas Wiebe also discussed German developments in the field of the protection of image as a personality right, data protection in employment as well as the right to be forgotten in the interpretation of the Federal Constitutional Court. With regard to the right to be forgotten, he mentioned cases (Right to be Forgotten I and Right to be Forgotten II) which navigate the relationship between national and constitutional law and European fundamental rights. He noted that in the aftermath, if a field of the law had not been completely harmonised and there are differences in the Member States, the Constitutional Court will review national law mostly in light of national fundamental rights even if European fundamental rights apply simultaneously (Right to be Forgotten I). However, in cases where there is a full harmonisation, the Court ruled it has the competence to apply EU fundamental rights in cases where their interpretation is clear (Right to be Forgotten II). He noted these cases are a manifestation of "how the Federal Constitutional Court manages not be forgotten".

There have also been developments on the interpretation of the data subjects' rights, e.g., right to be informed, and right to restriction of processing. Importantly, recent caselaw shows that, e.g., a breach of data protection law is not sufficient for damages and that the effect on personality has to be proven by the dependant (LG Darmstadt, 26.05.2020 13 O 244/19). He noted that there is a general tendency to believe that a data protection infringement is as not sufficient to establish harm, but there has to be some evidence.

In conclusion, Andreas Wiebe pointed out to a growing concern that the enforcement of the GDPR will be handled differently in different Member States thus leading to disadvantages in competition for companies. In the perspective of the near future, there are some key legislative desires, e.g., clarifying data protection in telemedia and telecommunications, or providing a coordinated proposal for implementing Art. 91(1) GDPR within the competence of the federal level in close coordination with the states. He also believes that the mentioned preliminary question on the GDPR, as well as the forthcoming adoption of the Directive on consumer collective action will pave the way for the effectiveness of enforcing the GDPR. Overall, he believes improving a common public discussion, both in the general public as well as the professional field, could also help improve the implementation process. In this context, there is a need for more comparative work to improve the development of data protection law, to which the Series already contribute.