Bloomberg Law

Privacy and Security Law Report®

Legislation

An English-Language Primer on Germany's New GDPR Implementation Statute Part 2: Individual Rights, DPA Oversight and Enforcement, and Litigation

Legislation

This is Part 2 of a two-part English-language overview of Germany's recently passed new version of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, or BDSG)—the BDSG-New, which implements the EU General Data Protection Regulation (GDPR). Part 1 focused on internal-facing compliance provisions. This part focuses on individual rights, privacy regulator oversight, and litigation.

By Daniel Felz

On July 6, Germany implemented the European Union General Data Protection Regulation (GDPR) with the passage of a statute titled the Data Protection Amendments and Implementation Act. The Act repeals Germany's venerated Federal Data Protection Act (Bundesdatenschutzgesetz, or BDSG) and replaces it with an entirely new BDSG, aptly referred to as the ''BDSG-New.'' Germany becomes the first EU Member State to pass a GDPR implementation statute. Given Germany's reputation as one of, if not the, most serious privacy jurisdiction in the EU, the BDSG-New is a critical piece of legislation for companies with EU operations.

The following represents an overview of the BDSG-New for English-language audiences. While focusing on the more salient provisions of the statute, I have attempted to provide insight into the drafting history and debate that helped shape the BDSG-New's final form.

Given the breadth of the statute, this overview proceeds in two installments. This part focuses on individual rights, data protection authority oversight, and litigation.

Daniel Felz is an attorney at Alston & Bird LLP in Dallas, TX and Brussels, Belgium. He is a member of the firm's privacy & data security team.

Individual Rights A central part of the GDPR is the new and expanded rights provided to individuals under Articles 13 to 22. The BDSG-New introduces a number of significant limitations on GDPR rights:

Information Rights. Articles 13 and 14 of the GDPR require companies to provide expanded privacy notices to EU individuals. The BDSG-New provides potentially significant exemptions to information obligations when confidential data is involved. German law defines confidential data as any data that, ''pursuant to a provision of law or due to their nature, must be kept confidential.'' When companies collect data from sources other than the affected individual, Section 29 of the BDSG-New exempts companies from providing notice to the extent doing so would reveal confidential information. Companies providing network security services may find this exemption useful.

Access Rights. Article 15 of the GDPR permits individuals to access any personal data that a company holds about them. The BDSG-New creates exemptions for German data regarding:

- Confidential Data. Current German law exempts companies from providing access to the extent doing so would reveal confidential data, and the BDSG-New maintains this exemption (with confidential data again

 ISSN 1538-3423

defined as data that, ''pursuant to a provision of law or due to their nature, must be kept confidential''). German law contains a number of statutory duties of confidentiality that may justify withholding data. One remaining question is whether contractual non-disclosure language creates ''confidential data'' that can be withheld from access requests. The German Chamber of Public Accountants (*Wirtschaftsprüferkammer*) asked the German legislature to clarify this issue, but the final BDSG-New remained silent.

■ High-Cost Fulfillment. The BDSG-New drafts initially contained broad exemptions that would have permitted companies to deny access requests when they endangered a ''generally recognized business purpose.'' In its final version, Section 34(1) narrowed this exemption, but maintained significant carve-outs. Companies do not have to provide access to:

- archived data (defined as data that are ''stored only because, due to legal or statutory retention provisions, they cannot be deleted''); or
- data stored exclusively for purposes of data safeguarding (e.g., backups) or data protection audits.

To claim these exemptions, companies must implement appropriate measures that ensure the data cannot be processed for any other purposes. Also, companies need to document their decision to rely on the exemption, and must explain the exemption to individuals when responding to access requests.

Automated Decisions. Whenever companies employ algorithms that have legal effects or ''significantly affect'' individuals, Article 22 of the GDPR generally requires them to obtain prior opt-in consent and offer human appeal mechanisms. Still, the GDPR permits Member States to pass laws exempting automated decisions from these requirements. During public comment, one of Germany's largest insurance associations (*Gesamtverband der Deutschen Versicherungswirtschaft*) asked that the BDSG-New support efforts to digitalize claims processing. Section 37 of the final BDSG-New created exemptions for automated decisions in the insurance context, as follows:

- decision-making algorithms do not need consent and appeal mechanisms if the individual receives everything he or she is asking for; and
- in health insurance, no prior consent is necessary for automated decisions based on binding fee-for-service tables (but if the individual receives a partial denial, the insurer must provide a human appeal mechanism).

Breach Notifications to Individuals. The GDPR places companies under an obligation to notify affected individuals whenever a data breach creates a ''high risk'' for their privacy that cannot be sufficiently mitigated. The BDSG-New introduces the first Member State exception to notification duties. Under Section 29(1) of the BDSG-New, companies do not have to notify individuals of personal data breaches to the extent that doing so would reveal confidential data.

Still, the BDSG-New requires companies in breach situations to weigh confidentiality interests against individuals' interests and to notify affected individuals if their interests predominate. Notification should ''particularly'' be made ''in light of impending harm.'' The statute does not specify harms that mandate notification; thus, the scope of this exemption may be uncertain until further guidance.

DPA Oversight One-Stop Shop, German Version. Germany is famous for its 17 data protection authorities (DPAs), one of which is federal and 16 of which are maintained by the German states (or *Länder*). The state DPAs are the DPAs of ''general jurisdiction,'' having supervisory authority over almost all private companies. The federal DPA has jurisdiction over telecommunications and postal-service companies. Since the state DPAs are the primary supervisors of private enterprise, companies with multiple German locations have found separate locations subject to different German DPAs.

The GDPR introduces a ''one-stop shop'' mechanism at the EU level, and during drafting, the Upper House of Parliament suggested that a similar mechanism should be available within Germany. The BDSG-New adopted the suggestion. If a company has multiple German establishments, the DPA with jurisdiction over the company's ''main establishment'' can serve as the company's lead DPA within Germany. If the German DPAs disagree about who should be the lead DPA, they must resolve the matter among themselves. Having a ''lead'' German DPA could substantially simplify German privacy compliance for companies with multiple German locations.

Confidentiality and Privilege in DPA Investigations. Article 90 of the GDPR permits Member States to ''adopt specific rules to set out [DPAs'] powers'' concerning controllers subject to ''obligation[s] of professional secrecy.'' This article gave rise to one of the BDSG-New's most debated provisions. Early BDSG-New drafts largely eliminated DPAs' powers to investigate ''professional privilege carriers'' (*Berufsgeheimnisträger*)—such as attorneys, accountants, and doctors. This led Germany's Federal DPA to contend that the legislature could not restrict its ability to investigate any data controller it wished. Public comment showed attorneys and accountants raising arguments in the opposite direction. The Institute of Public Auditors (*Intsitut der Wirtschaftsprüfer*) pointed out that professionals cannot waive privilege. The German Bar Association (*Bundesrechtsanwaltskammer*) even offered to serve as a sector-specific privacy supervisor for all 164,000 licensed attorneys within Germany (a proposal that was not accepted).

The final version of the BDSG-New maintains significant limits on DPA investigatory powers. Section 29(3) states that German DPAs do *not* have the power to access personal data held by privilege-carrying professionals, or to conduct on-site inspections at professionals' offices, to the extent that these measures would lead to violations of professional secrecy or confidentiality. The statute also extends this exemption to professionals' IT vendors.

This exemption potentially provides professional advisory firms with a basis for resisting significant portions of DPA investigations. Still, German DPAs are likely to challenge this exemption where possible—the Berlin DPA has already issued a statement arguing that the exemption exceeded the German legislature's powers.

DPA Fines. Present German law contains a multitiered fining regime, differentiating between what can

   ISSN 1538-3423

be described as ''formal'' violations—finable up to 50,000 euros ($59,452)—and ''substantive'' violations, which can be fined up to 300,000 euros ($356,715). German law also permits fines to match any profit a company has received from wrongdoing. A famous example occurred when the DPA of Rheinland-Pfalz fined insurance company Debeka 1.3 million euros ($1.55 million) for operating a ''lead generation system'' in which it paid public employees ''fees'' to forward new hires' contact information.

The BDSG-New abolishes the fine levels of present German law, indicating in commentary that the GDPR now comprehensively regulates fine levels. (Section 43 of the BDSG-New does permit 50,000 euro ($59,452) fines for violating consumer credit disclosure obligations, but this implements the EU Consumer Credit Directive and is outside the GDPR's preemptive ambit.)

As many companies are aware, the GDPR increases fine potential to up to 4 percent of annual worldwide turnover. One question for Germany is how extensively its DPAs will make use of their increased fining powers. Some German DPAs have been hesitant to issue fines; the DPA of Nordrhein-Westfalen has previously stated that it views fines as the ''last resort.'' Still, recent years have seen German DPAs issue their first fines exceeding 1 million euros ($1.19 million). Additionally, the Bavarian DPA recently stated it reads the GDPR as *requiring* fines whenever a violation is discovered—the only remaining question is how high fines will be.

Some companies have inquired about what factors go into calculating a fine. The Berlin DPA recently provided guidance that the duration of the violation, the types of data affected, whether the violator received financial benefits, and cooperativeness will affect fining levels. Importantly, self-reporting could result in lower fines.

Another important question is how GDPR fines will interact with German rules on imputing liability to companies. The BDSG-New provides that the Act on Regulatory Offenses governs German DPAs' assessment of fines. The Act is often used as a basis for imputing liability for employee misconduct to organizations. However, unlike the U.S. *respondeat superior* doctrine, the Act only imputes liability when *top-level managing employees*, such as executives, either commit wrongful acts, or negligently supervise subordinates. The Berlin DPA has already pushed back against limiting fines in this fashion, arguing that the GDPR adopts EU antitrust law's ''functional'' approach to imputed liability – i.e., an employee who commits a wrongful act while acting within his assigned ''function'' imputes liability to the company – which more or less tracks the U.S. *respondeat superior* doctrine. Some German commentators have already lined up on the other side, and companies that are fined based on their employees' actions will have materials to support non-frivolous challenges.

Many companies have asked whose revenue serves as the basis for the 2 percent or 4 percent sanctions—the parent, the German subsidiary, or both? The GDPR suggests that the concept of an ''undertaking'' contained in the EU treaties governs this question. The Berlin DPA thus argues that the GDPR adopts EU antitrust law's ''economic unit'' approach to sanctions. Thus, in the Berlin DPA's words, ''if a subsidiary violates data protection provisions, its revenues *together with those of its parent corporation* constitute the basis for assessing fines.'' Recently, all federal and state DPAs in Germany released a similar joint statement: ''parent and subsidiary are viewed as an economic unit, so that their combined turnover is the basis for calculating fines.'' Here also, commentators are lining up on both sides of the issue, and a company that receives a significant fine may find a challenge merited.

Challenging DPA Actions. German procedural law is bifurcated when challenging DPA action. This arises from what commentators have described as the ''competing'' goals of DPA activity. DPAs are supervisors who can use state-granted coercive powers to order changes in how companies process data. On the other hand, DPAs can issue fines, which does not itself change companies' behavior, although companies often elect to change behavior in response.

These differing goals are supported by different procedures. ''Supervisory'' DPA action will result in an administrative order to perform (or refrain from) certain actions – a recent example occurred when the DPA of Hamburg prohibited WhatsApp data from being transferred to Facebook. Supervisory actions are conducted via administrative proceedings (*Verwaltungsverfahren*) whose results can be challenged in Germany's administrative courts, which are a specialized court system separate from Germany's ordinary civil courts.

In contrast, DPAs' assessment of fines occurs through procedures set forth in the Act on Regulatory Offenses (*Gesetz über Ordnungswidrigkeiten*). Proceedings under the Act are quasi-criminal in nature and result in a ''Fine Notice'' (*Bußgeldbescheid*). Companies have a right to object to the Notice, and if they do, the evidence is first forwarded to the public prosecutor. If she deems the evidence credible, the challenge is placed before the local magistrate court (*Amtsgericht*) for review. The courts that review fines are *not* administrative courts, but rather the ''ordinary'' courts of general jurisdiction.

The BDSG-New maintains this bifurcated structure. For ''supervisory'' orders, Section 20 maintains the administrative courts as a forum for challenges. For fines, the BDSG-New maintains the Act on Regulatory Offenses, although a late amendment to Section 41 ensures that if a fine is over €100,000, challenges are not heard by a magistrate, but by the district court (*Landgericht*) above it. This appears to recognize the seriousness of GDPR fine potential.

DPA Challenges to International Transfer Mechanisms. Last year, I reported that German DPAs had demanded statutory standing to challenge decisions of the European Commission, such as the EU-U.S. Privacy Shield. Their proposals were tabled when the Interior Ministry indicated that the BDSG-New would address the issue.

The final Section 21 of the BDSG-New grants DPAs a limited right to challenge EU Commission decisions. A DPA must first encounter a Commission decision ''whose validity is determinative'' for its decision. It may institute a challenge before Germany's Supreme Administrative Court (SAC). If the SAC believes the Commission decision is lawful, it may issue a final decision and dismiss the DPA's challenge. But if the SAC shares the DPA's doubts, it must refer the case to the European Court of Justice for review.

These standing rights went into effect immediately. However, given that Digital Rights Ireland has already filed a challenge to Privacy Shield before the EU courts,

German DPA challenges may be unlikely in the near term.

Litigation Germany is not traditionally a plaintiff-friendly jurisdiction. Without discovery or collective proceedings such as class actions, and with losing parties bearing the full cost of proceedings—including attorneys' fees—Germany can be challenging for plaintiffs. For individuals, German filing fees can be a significant hurdle, since they rise with the amount in controversy—for example, a 100,000 euro ($118,905) civil claim could require around 12,000 euros ($11,890) in filing fees (although legal aid is available in limited circumstances).

In Germany, data-protection law suffers a particular dearth of case law. Commentaries abound and the privacy community is vocal, but few data-protection cases have proceeded to a court decision. Also, much of significant recent litigation has been ''defendant-driven'' administrative litigation by companies challenging DPA measures, not damages suits brought by individuals against companies.

The BDSG-New cannot itself introduce a sea change to present German practice, but it does work within the GDPR framework to ensure that aggrieved individuals have avenues to redress under a reduced burden:

Special Jurisdiction and Service Provisions. Article 79 of the GDPR provides a new special jurisdiction rule giving German courts jurisdiction over individuals' privacy claims when the defendant-company has an establishment in Germany, or when the aggrieved individual resides in Germany. Additionally, if the defendant-company has no EU presence—but has appointed an EU representative as required by the GDPR—Section 44 of the BDSG-New deems the representative authorized to receive service of privacy suits. This can obviate a need for plaintiffs to resort to international or substituted service.

Expanded Damages. Article 82(1) of the GDPR will permit individual claimants to recover ''non-material damage'' for privacy violations. This expands the German liability regime, which previously only awarded actual losses. For example, the GDPR suggests that the mere ''loss of control over . . . personal data'' or ''unauthorized reversal of pseudonymization'' may be sufficient to trigger awards for ''non-material'' damage. If so, this would provide for more readily available damage awards than the jurisprudence of some U.S. circuits.

Strict Liability? Traditional problems of proof may also be lessened. Article 82 of the GDPR is structured so that companies are presumably liable for privacy violations as soon as they are ''involved in'' processing, but may rebut this presumption by showing they are not in any way ''responsible'' for harm to the plaintiff. Some German commentators have suggested that this introduces no-fault liability for privacy violations. As a result, German plaintiffs would need only show that a company is ''involved in'' processing in order to recover from the company; it would then be the company's burden to show it bears no fault for any privacy violations.

Class Actions? In January 2016, I reported that the German legislature had granted consumer-protection organizations new statutory standing to pursue injunction class actions against companies for data protection violations. That legislation remains unaffected by the BDSG-New. As a result, German consumer organizations may attempt to cease-and-desist how companies are processing data, backed up by a threat of an injunction suit.

Still, Germany maintains no collective mechanism for seeking damages akin to what U.S. plaintiffs can achieve via Rule 23 or multidistrict litigation. When multiple German plaintiffs want to collectively assert similar claims against a defendant, they sometimes assign their claims to a special purpose vehicle, which appears before court as a single plaintiff. This approach is not without risk; German statutes prohibit making a business of soliciting and asserting third-party claims. For example, in Austria (which has a similar legal system), Max Schrems is attempting to receive assignments of individuals' claims to assert them against Facebook—and as I reported, one issue is whether he is prohibited from receiving the assignments because he is operating a business.

Article 80 of the GDPR attempts change the situation to some degree. It permits individuals to ''mandate'' nonprofit consumer-protection organizations with asserting their rights in court, essentially permitting consumer organizations to bring opt-in class actions. The individual plaintiffs would not be assigning their claims to the nonprofit, but instead be represented by the nonprofit. Although nonprofits do not have the right to ''receive compensation'' on plaintiffs' behalf, they can still obtain collective liability determinations. Still open, however, is whether organizations can actively *solicit* privacy claims from individuals.

Suits Against DPAs. Article 78 of the GDPR provides that individuals have a right to bring an action against DPAs to challenge any ''legally binding decision,'' or whenever DPAs do not take action on a complaint within three months. Section 20(1) of the BDSG-New confirms that the German administrative courts are open to all ''disputes between a natural or legal person and a federal or state DPA.'' Such a suit can have the effect that a mandamus action in U.S. courts would have, and as an example, the *Schrems* litigation that invalidated Safe Harbor began as a suit against the Irish DPA.

BY DANIEL FELZ

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

  PVLR ISSN 1538-3423