Bloomberg Law

Privacy and Security Law Report®

Legislation

An English-Language Primer on Germany's New GDPR Implementation Statute Part 1: The Scope of the Statute and Internal Compliance Duties

German GDPR Legislation

This article is the first in a two part series on Germany's new data protection law, the first in the EU to add changes to reflect the new European Union General Data Protection Regulation privacy regime. In Part 1, the author focuses on insights for companies from the drafting history and scope of the new German law, as well as on important internal-facing compliance issues addressed by the statute: reuse of information, appointment of data protection officers, and implementation of employee privacy rules.

By Daniel J. 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 BDSG-New has a fascinating history involving more debate and controversy than many observers may expect from Germany. Initially, the German government crafted the BDSG-New as a sweeping new privacy regime that would have allowed unrestricted Big Data uses, as well as substantial restrictions on individuals' privacy rights. This resulted in pushback from privacy advocates and from Germany's federal and state data protection authorities (DPAs) tasked with supervising privacy laws. At the same time, industry groups weighed in to challenge provisions they saw as onerous for businesses. After rounds of drafting and debate, Germany settled on a more modest approach that makes some changes, but preserves a number of existing rules. Lawmakers may have been moved by considerations that—as the former head of Germany's Federal DPA put it—''we have a reputation to lose,'' and that the BDSG-New would set precedents for other Member States.

Still, the BDSG-New contains a number of new or modified provisions that companies will find significant. I followed the BDSG-New from start to finish, beginning when an initial draft was leaked to the German press in September 2016. Along the way were three additional drafts of the statute, numerous statements filed with ministries and the German legislature during rounds of public comment, and committee hearings with testimony from experts from across Germany.

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 at-

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.

 ISSN 1538-3423

tempted 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. Today it focuses on the drafting history and scope of the BDSG-New, as well as on important internal-facing compliance issues addressed by the statute: reuses of data, data protection officers, and employee privacy rules.

Drafting History The public nature of the BDSG-New's drafting may provide avenues for statutory interpretation and arguments before German DPAs and courts. The BDSG-New was drafted by Germany's Interior Ministry (*Bundesministerium des Innern*, or BMI). The BMI is one of Germany's most important cabinet ministries, responsible for internal security, federal police, and aspects of national security. For U.S. readers, a comparison could be Homeland Security working with the FBI to draft a comprehensive data protection statute.

By August 5, 2016, the BMI had completed an initial secret internal draft of the BDSG-New. This draft was leaked to the German press—along with formal comments from Germany's Justice Department, Federal DPA, and 16 state-run DPAs. The comments revealed significant pushback from the DPAs on secondary data uses and restrictions to individual rights. They also showed the Justice Department had prevented the BMI draft from proceeding to the legislative process until certain changes were made.

In mid-November 2016, the BMI published an updated draft containing significant revisions, but still containing fundamental changes to German privacy law—such as permitting companies to make any secondary use of data supported by what they considered to be their ''legitimate interests.'' The BMI then announced a two-week period for public comment. Following this initial round of comment, the BMI amended a number of the more debated portions of the draft BDSG-New and presented the amended draft to the federal cabinet of ministers.

On Feb. 1, the cabinet approved an amended draft (in German), which was introduced as a bill in the German legislature. When the BDSG-New entered the Lower House (*Bundestag*), its Committee on Interior Affairs held a second two-week round of public comment, and a hearing for subject-matter experts to present positions. The committee then made several significant final amendments before re-introducing the bill to the full legislature, which passed it in May. After the Federal President signed the bill, it was published in Germany's *Federal Register* on July 5. The BDSG-New is thus an enacted statute, but—like the GDPR—almost all of the BDSG-New will not enter into force until May 25, 2018.

Extraterritorial Scope The GDPR expands the extraterritorial scope of EU privacy law. Article 3 of the GDPR not only subjects companies with an EU presence to EU privacy law, but also any company *outside* the EU that ''offer[s] goods or services'' to EU residents, or monitors EU residents' behavior. However, early drafts of the BDSG-New maintained German privacy law's traditional territorial approach, limiting the BDSG-New to companies with a German establishment. This potentially had the consequence of subjecting companies using German data to the GDPR, but not to German law.

By the time of its passage, however, the BDSG-New had expanded beyond German borders. Under Section 1(4) of the BDSG-New, a company is subject to the BDSG-New to the extent that it:

- processes personal data within Germany;
- processes personal data in the context of the activities of an establishment within Germany; or
- does not have an establishment within the EU, but falls within the GDPR's extraterritorial scope of application—such as by offering goods or services to EU residents, or by profiling EU residents online.

The final prong establishes as a new rule that, if a non-EU company is subject to the GDPR, it is automatically subject to German data protection law. This rule may represent an attempt to ensure that German law, and German DPA supervision, can apply to non-EU companies as soon as they begin processing German data. Still, the rule may have unforeseen consequences in that it potentially subjects companies to German law in the absence of any factors connecting them to Germany—a Florida company marketing to Spanish residents would be in-scope for the GDPR, and thus technically within the scope of German privacy law. Also, the rule may present challenges when a U.S. company is processing data of, for example, both German and French residents—especially if France and other EU Member States adopt the same rule.

Still, a German DPA's determination that German law governs particular operations is not binding on German courts, which review applicable-law determinations *de novo*. In fact, in several recent challenges to DPA rulings, courts at least partially reversed the DPAs' decision to apply German law.

Reuses of Data One of the most debated topics during BDSG-New drafting was how much freedom companies should have to make new secondary uses of data they hold. Chancellor Angela Merkel stated that Germany should ''not make everything so restrictive again'' such that ''big data management isn't possible after all.'' A November 2016 BDSG-New draft would have permitted companies to make any secondary use of data that was ''necessary to pursue the controller's legitimate interests''—regardless of the effects on individual privacy—thus letting business models determine permitted secondary Big Data uses. This provision evoked resistance from privacy advocates.

The final BDSG-New takes a more moderate approach. Section 24(1) only permits companies to make secondary use of data for ''the establishment, exercise, or defense of civil claims.'' This sounds like what companies are already permitted to do, but it is arguably more restrictive. Secondary litigation use often involves companies collecting and reviewing employee data for use in U.S. pretrial discovery. The BDSG-New will restrict companies' ability to do this to ''*civil* claims,'' raising questions as to how far companies can review German data in response to U.S. criminal or administrative subpoenas. As a practical matter, this may require work with works councils and amendments to works council agreements.

New Regime for Health Data In contrast, the BDSG-New introduces new permissions for companies to use health data. Article 9 of the GDPR generally requires companies to obtain prior opt-in consent to process

  PVLR ISSN 1538-3423

health data, but also permits Member States to pass legislation permitting processing without consent to serve public health interests.

The BDSG-New implements this provision. Relevant to biotechnology, pharmaceutical, and medical-device companies, Section 22(1)(1)(c) of the BDSG-New permits health data to be processed ''to ensure high standards of quality in the health care industry'' and ''for medicinal products and medical devices.''

As an example, medical device manufacturers may benefit from this provision. Newer medical devices often rely on feedback loops of device-generated data between the device, care providers, and device manufacturers. Increasingly—including in Germany—regulators require manufacturers to monitor devices and report incidents. Current law can require patients to enter into detailed consents, revocable at will, and it can be challenging for the multiple entities involved to manage consents and withdrawals. Section 22 would appear to move towards a more integrated regime for device-generated data, which may permit uses beyond treatment—e.g., monitoring, improvement, and reporting—in the interest of improving public health.

Importantly, Section 24(2) of the BDSG-New also permits secondary uses of health data without consent for medicinal products and medical devices, presumably meaning that companies can use their existing German data to start. In exchange, the BDSG-New requires companies to implement ''suitable and specific'' safeguards, listing 10 safeguards that DPAs will likely expect to see in place, such as employee training, access controls, encryption, pseudonymization, and security audits.

Data Protection Officers Data protection officers (DPOs) are a German institution. They were originally introduced as a hybrid strategy for supervising privacy compliance: instead of informing government supervisors about every aspect of their processing, companies were exempted if they internally appointed a DPO responsible for supervision. While other Member States left DPOs largely optional, Germany mandated their appointment in practically every business with 10 or more employees. Over time, DPOs became an integral part of German privacy practice.

The GDPR adopted a compromise position on DPOs. Article 37(1) of the GDPR requires companies to appoint a DPO only if their ''core activities'' involve ''large-scale'' (a) processing of sensitive data or (b) regular and systematic monitoring of EU residents. At the same time, the GDPR permits EU Member States to pass their own statutes requiring DPOs to be appointed in additional circumstances. The BDSG-New does just that, electing to maintain and expand Germany's DPO tradition:

■ Duty to Appoint: Section 38 of the BDSG-New requires companies to appoint a DPO whenever:

- they employ at least 10 people whose regular duties include processing personal data;
- their ordinary business includes processing data for purposes of selling the data or transferring the data anonymously, or for market or opinion research; or
- they conduct processing that requires a data protection impact assessment (DPIA) under Article 35 of the GDPR.

The last requirement is new and may be of interest because if a company anticipates conducting a DPIA, it must have a DPO in place if it is using German data—in fact, under existing regulatory guidance, the DPO should be consulted for every material aspect of the DPIA. At the same time, almost any company with a German presence will have 10 employees, and for these companies—to paraphrase the Bavarian DPA—not much will change.

■ Protected Employment: As has been the case to date, German DPOs cannot be fired unless employers can show facts that would permit the employee's immediate termination for cause. Additionally, DPOs' protected status continues for a year after the DPO has left the DPO position.

■ Protected DPO Status: In addition to employment, the DPO's *status as DPO* is protected. A DPO cannot be removed from her position as DPO—even if she is not fired—unless facts analogous to those that would permit immediate for-cause termination are present.

■ New Standard for DPA Activity: To date, German statutes have required DPOs to ''*work toward* compliance'' with privacy law within their organizations. Article 37 of the GDPR will now require DPOs to ''monitor compliance.'' Given decades of German practice, this may be a distinction without a difference, but it also may set a new baseline for acceptable DPO behavior.

Additional German requirements for DPOs are expected to come from DPA guidance. For example, the GDPR permits corporate groups to appoint a single group-wide DPO. German DPAs have already stated that they expect any such ''global'' DPO to sit within the EU, unless companies can document she would be more effective from the group's headquarters. Additionally, a global DPO needs to be ''readily available'' for German DPAs, employees, and third-party data subjects, potentially via a hotline or web form, and must have the resources to communicate in German.

Employee Privacy Rules At present, Germany's law of HR privacy primarily comes from Section 32 of the current BDSG, provisions of other employment-related statutes (such as the Works Constitution Act [*Betriebsverfassungsgesetz*], which provides for works councils), and court decisions. Similarly, the BDSG-New contains one section dedicated to ''Processing for Purposes of the Employment Relationship.'' Still, the BDSG-New's Section 26 introduces a number of statutory provisions that do not currently exist in German law. Among the more salient are:

■ *General Rules Stay Intact*. Current German law contains a general permission to process employee data for the establishment, performance, or termination of the employment relationship. Section 26(1) of the BDSG-New similarly generally permits processing of employee data as is ''necessary for purposes of the employment relationship.'' ''Necessary'' under the statute does not mean strictly necessary, but rather ''striking a practical balance'' between ''the interests of the employer'' and ''the employee's privacy rights.'' This reflects the case law of German labor courts and grants companies and employee representatives flexibility in tailoring processing to their organizations.

■ *Works Council Agreements Remain, but Renegotiation Necessary*. German labor court decisions have

long permitted companies to process data on the basis of works council agreements. The BDSG-New maintains the state of the law, stating in commentary that ''works council agreements . . . may continue to constitute a legal basis for rules on employee data protection.'' At the same time, however, Article 88(2) of the GDPR creates new requirements for works council agreements, mandating that they include ''suitable and specific measures'' to safeguard ''the data subject's human dignity . . . and fundamental rights,'' particularly regarding (a) transparency, (b) data transfers within corporate groups, and (c) ''monitoring systems at the workplace.'' Many existing works council agreements will lack such provisions, and both the GDPR and BDSG-New indicate the agreement's validity may depend on including them. The statute contains *no exemption* for works council agreements concluded before its passage.

■ *Core GDPR Principles*. In exchange for granting companies flexibility to customize processing rules, the BDSG-New requires any HR processing framework to guarantee that ''core'' privacy principles will be observed. Section 26(5) requires all controllers to implement ''suitable measures'' to ensure that in all processing of employee data, the principles of Article 5 of the GDPR are complied with, including (a) purpose limitation, (b) transparency, (c) lawfulness of processing, (d) data minimization, (e) accuracy, (f) storage limitation, (g) confidentiality, and (h) integrity/security. Essentially, Section 26(5) makes reference to these principles a mandatory part of any works council agreement or internal HR policy.

■ *Statutory Recognition of Consent*. German law formally permits employees to consent to processing of their data, but German DPAs are traditionally skeptical that employee consents are voluntary. The BDSG-New gives a nod to this policy, stating that the validity of employee consent should ''especially'' be evaluated in light of the ''dependence of the data subject that exists in the employment context.'' However, Section 26(2) also introduces new scenarios in which employee consent can be considered voluntary and thus effective: when the employee receives an economic or legal benefit by consenting, or where the interests of the employee and employer are aligned. The statute provides further guidance on these consent scenarios:

- an ''economic benefit'' that can support consent is present when a company introduces an occupational health management program, or permits private use of company IT systems. The latter point may be relevant to companies asking employees for consent to monitor their private email and internet use, so as not to run afoul of German telecommunications secrecy laws;
- ''aligned interests'' are present when the company and employees work together to add employees to a company birthday list, or to use photographs of employees for an internet website.

■ *Sensitive Data Processing Without Prior Consent.* Often, companies with German employees must process sensitive data, such as health data for insurance purposes. Section 26(3) of the BDSG-New provides that employers can process sensitive data about employees to manage the employment relationship, or to exercise rights or fulfill duties of employment law or social-services law—so long as the employee does not have overriding privacy interests. To take advantage of this new exemption, companies will need to document sensitive data they are processing and why their interests outweigh those of employees.

■ *Employee Monitoring Rules Stay in Force*. Companies based outside the EU sometimes operate under the presumption that employees have no expectation of privacy in their use of corporate IT assets, and can thus be surprised by the restrictions on employee monitoring in Germany. The BDSG-New largely maintains Germany's current regime, which only permits employees to be monitored when the company can document reasons to believe the employee is engaged in serious breaches of duty or criminal conduct. In practice, works council agreements often set rules and procedures, such as consulting with HR and the works council before conducting anything beyond spot testing, pseudonymizing initial results, and restricting who can reidentify data. Additionally, companies should be aware that works councils have co-determination rights over any technology that *could be* used to monitor employees – such as data-loss applications – regardless of whether the technology is actually intended for that purpose.

By Daniel Felz

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

  PVLR ISSN 1538-3423