# Less Than 20 Weeks to the European Union GDPR—What to Do Now?

*By Lothar Determann*

As we are wondering what 2018 will bring, we have known one fact since 2016: May 25, 2018 is the day when the European Union General Data Protection Regulation (2016/679/EU) (GDPR) will take effect.
This is the first significant update of data protection laws in Europe for more than 20 years. In 1995, when the then-called European Community (EC) enacted the Data Protection Directive (95/46/EC), it only harmonized existing national laws. It hardly updated the national data protection laws, which member states had been enacting since 1970. The current EU data protection laws are from an ancient time before the internet, smart phones, cloud computing, virtual worlds, big data, artificial intelligence and Pokemon. Apart from attempts to lower and then heighten again consent requirements for web cookies in 2002 and 2009 respectively, European data protection laws have remained largely unchanged and outdated.

But this year, data protection laws in Europe are changing with a vengeance—including draconian penalties of up to 20 million euros ($23.91 million) or 4 percent of total annual worldwide turnover, whichever is higher. Most companies have been working on updating their compliance programs for more than a year. Approaches and progress vary greatly, but the following questions are frequently asked:

**What Can Companies Expect to Happen on May 25, 2018?**
Data protection authorities have announced that they will conduct more routine audits. For example, the data protection authority in the German state of Bavaria mailed aGDPR questionnaire already in May 2017 to 150 randomly selected companies and publicly announced that all companies in Bavaria—where many multinationals maintain subsidiaries—should have their answers ready by May 25, 2018.

**Can Companies Count on a Transition Period or Initial Leniency?**
Some degree and period of leniency would be appropriate, given the dramatic increase in requirements. Particularly companies outside the European Economic Area (EEA) should be afforded extra time to process the 173 recitals and 99 articles on 88 pages of regulations (more than four times the page count of Directive 95/46/EC in the Official Journal)—plus national laws and official guidance that the 28 member states continue to issue on a daily or weekly basis, often only in one of the less commonly used of the 24 official EU languages.

But, companies should probably not count on a formal transition period, given that the EU published the final, binding text of the GDPR already in May 2016 with a two year delayed application date to give companies time to adjust (Art. 99). Since 2016, EU

institutions and national data protection authorities have been actively communicating about the upcoming application date and issuing guidance.

**Which Data Protection Authority's Guidance is Relevant for My Business?**
Multinationals have to observe guidance from each data protection authority in whose territory they maintain a subsidiary. Companies without any subsidiaries in the EEA should pay particular attention to the guidance of the data protection authority in charge of the territory where they appoint a legal representative (per Art. 27 GDPR), but they may hear from data protection authorities in other EEA member states, too. According to the GDPR, a "lead authority" has jurisdiction over each controller and processor per Art. 56 *et seq.* and recitals 124 *et seq.* Within a multinational group of companies, each subsidiary qualifies as a "controller" and "processor" and is thus subject to separate jurisdiction. Some EEA member states have appointed one authority for their entire country (*e.g.*, French regulator, the CNIL and the U.K.'s Information Commissioner's Office). Others have appointed separate authorities for each province or state within a country (*e.g.*, Germany has 16 authorities, one in each of its 16 Bundeslander).

**Will Data Protection Law Enforcement Increase in the EU?**
Probably yes. Most data protection authorities have announced plans for more audits and sanctions and some have already increased proceedings in the last few years. The next years may bring a few high profile cases against "trophy targets" (which will tie up a lot of resources in litigation) and a flood of actions against "low hanging fruit"-type formal violations to fund the authorities' extended operations and resources, similar to "traffic ticket" type-enforcement. Every company should focus on presentable compliance paperwork to avoid standing out as a "low hanging fruit" in an audit or response to a routine questionnaire.

**What are the Top 10 Compliance Priorities?**
Every business has a different risk profile and thus different priorities. Companies have to focus on more compliance priorities if they had prior run-ins with EU data protection authorities, experienced bad publicity around privacy topics, maintain employees or subsidiaries in the EEA, are subject to scrutiny by works councils, process consumer data, belong to regulated industries, or rely on data monetization. But even companies without any of these risk factors may be confronted with questions about GDPR compliance from corporate customers or in the context of data security breaches. The following top 10 compliance priorities seem relevant to nearly all companies with direct or indirect business ties to Europe:

• **Appoint privacy officer(s)** where required or beneficial; many companies are not strictly required under the GDPR to appoint a formal data protection officer, but may be subject to national law requirements or find it beneficial for various regulatory or operational reasons to appoint a local and/or global data protection officer, privacy

counsel or global privacy chief; in any event, you need to put someone in charge at the outset. *See* Determann's Field Guide to Data Privacy Law, 3d Ed. #1.1-1.15 (2017).

• **Upgrade and document your data security measures**—Including data retention/deletion rules, and technical and organizational measures that you require vendors to follow and that you can commit to contractually vis-a-vis customers, also to reduce the risk of costly security breaches, to comply with U.S. and other countries' data privacy laws, and to protect trade secrets.

• **Implement adequate data processing agreements with vendors**—Based on EU SCC 2010, Art. 28(3) GDPR, the Health Insurance Portability and Accountability Act of 1996, the Payment Card Industry Data Security Standard, and other regimes that may apply to your business. S*ee*, L. Determann, *EU Standard Contractual Clauses for Transfers Of Personal Data to Processing Service Providers Reassessed*, BNA Privacy and Security Law Report 10 PVLR 498 (2011).

• **Establish processes to grant data subject rights** and automate responses, including to data access, erasure, restriction and mobility requests (possibly on a geographically differentiated basis, per country or region, given that not all data subjects around the world expect such rights).

• **Prepare and keep up-to-date records of data processing activities** per Art. 30 GDPR for each legal entity and field of activity (*e.g.*, HR, customer data, marketing).

• **Document compliance with each applicable privacy principle and legal requirement in a dossier**, including data protection impact assessments and "data protection by design" analyses, to achieve, monitor and demonstrate accountability as required by Art. 5(2) GDPR and as a basis for internal training programs and defending against complaints.

• **Update your intercompany data transfer and processing compliance documentation**—The GDPR grandfathers existing European Commission decisions regarding countries' adequacy and Standard Contractual Clauses, but nevertheless requires updates to binding corporate rules, data processing agreements, consents and other mechanisms. See L. Determann, B. Hengesbaugh, M. Weigl, *The EU-U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options*, Bloomberg BNA Data Privacy & Security Law Report, 15 PVLR 1726, 9/5/16 (2016).

• **Update data privacy notices**—Including for your website (including "cookies"), mobile sites, customers, vendors, employees, job applicants, callers, marketing email recipients, and other data subjects.
• **Appoint a local representative** for entities outside the EU per Art. 27 GDPR.

• **Mind the ROW**—While you are comprehensively reviewing and upgrading your compliance program, use the opportunity to satisfy national law requirements in the EU as well as in the rest of the world (ROW), including U.S. federal and California state requirements. *See* L. Determann, California Privacy Law—Practical Guide and Commentary (2d Ed. 2017).

**What Common Pitfalls and Mistakes to Avoid?**

• **Document compliance, not violations**. Some companies have invested in elaborate "gap assessments" and voluntary "compliance audits" before they actually started upgrading their compliance programs. This can result in thoroughly documented compliance deficits, sometimes flagging violations of privacy law that have already been in effect long before the GDPR was enacted. Were internal audit departments and external consultants or auditors at work, attorney client privilege may not be available. Third party audits and validation are certainly recommended—but ideally after actually upgrading the company's compliance program, not before. Once a company has completed a formal gap assessment, it must expeditiously work on remedying all identified gaps.

• **Don't let perfect be the enemy of good**! Some organizations seem overwhelmed by the sheer size of the task and end up paralyzed. Yet, any opportunity to make concrete progress should be seized. Having some adequate data processing agreements signed is better than none. Every technical and organizational data protection measure can help prevent a data security incident.

• **Pick the right tools for your organization**. Some large and sophisticated organizations can benefit from using elaborate software tools to assess and document their compliance programs. Smaller companies may be better off using simple word.docx or spreadsheets to create records of processing activities or compliance dossiers.

• **Don't go crazy on data maps**—Art. 30 GDPR specifies clear requirements for records of processing activities. Above and beyond these formal requirements, companies need to understand all their data flows, retention and usage scenarios. Comprehensive and detailed data maps may be very helpful. But, before embarking on outsized data mapping exercises, in-house counsels and privacy professionals need to define limits for work product that they will be able to handle, including quite literally page limits for reports, to avoid drowning in voluminous documentation that they are unable to process.

• **Focus on statutory minimum requirements**. Some companies go above and beyond on certain requirements (*e.g.*, extra choices for data subjects, voluntary appointment of data protection officers, group-wide commitments to EU data protection laws, global data maps, worldwide coverage under EU SCC 2010, etc.). This can be vital for their business strategies, brand image, talent recruitment and customer relations. But, companies should start on "above and beyond" after—not before—they have satisfied

minimum requirements (*e.g.*, first obtain required commitments from vendors in adequate data processing agreements before extending "above and beyond" promises to customers). Unless and until in-house counsel is sure that all mandatory requirements can be satisfied in time, it is best to tackle mandatory requirements before the extras.

• **Pity your peers**—Go easy on your colleagues with questionnaires and questions; try to combine and synchronize compliance reviews as much as possible, e.g., under the GDPR, Privacy Shield, HIPAA, PCI DSS, etc.

• **Prioritize**—assess your organization's risk profile realistically and identify priority items; also, observe logical dependencies of tasks, e.g., internal records of processing activities should be the basis for external records of processing activities.

• **Don't miss an opportunity to address U.S. and other countries data privacy laws:** while you have the resources, attention and cooperation of the entire organization to work on GDPR compliance, do not miss an opportunity to address requirements under U.S. and many other privacy laws in other jurisdictions, which can often be conveniently satisfied in parallel.

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