This article has been published in
PLI Current: The Journal of PLI Press, Vol. 2, No. 2,
Spring 2018 (© 2018 Practising Law Institute),
www.pli.edu/PLICurrent.

PLI Current
The Journal of PLI Press
Vol. 2, No. 2, Spring 2018

GDPR *Ante Portas*: Compliance Priorities for the Impending EU Data Protection Regulation

Lothar Determann
Baker & McKenzie LLP

On May 25, 2018, the EU General Data Protection Regulation[1] will take effect, the first significant update of data protection laws in Europe in more than twenty years. In 1995, when the then-called European Community (EC) enacted the Data Protection Directive,[2] it only harmonized, but did not update, existing national laws, which member states had been enacting since 1970. The current EU data protection laws are from an ancient time before the Internet, mobile phones, cloud computing, virtual worlds, big data, artificial intelligence, and Pokémon. Apart from attempts to lower and then heighten again consent requirements for web cookies in 2002 and 2009 respectively,[3] European data protection laws have remained largely unchanged and outdated. But on May 25, 2018, data protection laws in Europe are changing with a vengeance—and draconian penalties of up to

EUR 20 million or 4% of total annual worldwide turnover, whichever is higher. Most companies have been working on updating their compliance programs for a while and revisited priorities at the beginning of 2018.[4]

The Road Ahead

During the final few weeks before May 25, 2018, companies need to take stock of what they have and have not yet accomplished with respect to their compliance programs and prepare for ongoing maintenance, updates and changes to their privacy compliance program and business. Companies have to brace for heightened enforcement activity in Europe (with potentially little or no extra transition period beyond the delayed effective date since the GDPR was enacted in May 2016). And they can expect many more new data-related laws: Most EEA member states are working on national legislation to supplement, complement, or implement the GDPR, even though the GDPR, as a regulation, applies directly to companies and does not require implementation, as the legacy directive did. Additionally, the ePrivacy Regulation, updating existing directives regarding privacy and electronic communications, including direct marketing and tracking technologies, is on the horizon. Also, the EU Commission and Germany are proposing "data ownership" legislation in an apparent attempt to soften the blow dealt to the EU information technology industry by the suffocating, prohibitive restrictions on data processing in the GDPR.[5] Argentina, Canada, Israel, New Zealand, Switzerland, Uruguay, and other countries whose data protection laws the EU Commission has found adequate may have to update their data protection laws to retain their status in the EU. And many other jurisdictions will watch the events unfold and debate whether they should follow the EU (including California, where a GDPR-like "California Consumer Privacy Rights Act of 2018" has been recently proposed).[6]

Priorities and Risk Factors

Every business has a different risk profile and thus different priorities. Companies that sell to other companies (as opposed to consumers) tend to be focused on satisfying customer demands more than statutory challenges. A U.S. company without any legal presence or customers in Europe may become subject to GDPR compliance attention only very indirectly. But, you may have relatively more priorities to focus on if your company:

- had prior run-ins with EU data protection authorities;
- has experienced bad publicity around privacy topics;
- maintains employees or subsidiaries in the EEA;
- is subject to scrutiny by works councils or other forms of collective employee representation in the EEA;
- processes consumer data from the EEA (particularly if you handle health information or other sensitive data);
- belongs to regulated industries; or
- relies on data monetization as a business model.

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.

Top Ten Priorities and Tasks

The following top-ten compliance priorities seem relevant to nearly all companies with direct or indirect business ties to Europe:

1. **Appoint privacy officer(s) where required or beneficial.** Not all companies are strictly required under the GDPR to appoint a formal data protection officer. But many companies find that their subsidiaries in the EEA may be subject to national law requirements to appoint a data protection officer, including companies with ten or more employees in Germany. Also, many businesses find it beneficial for various regulatory or operational reasons to appoint one or more local or global data protection officers, contact points, privacy counsel, or global privacy chief officers. In any event, regardless of titles, you need to put someone in charge at the outset.[7]
2. **Upgrade and document your data security measures.** Companies need rules on record retention and deletion to comply with data minimization and erasure requirements under the GDPR, and to avoid amassing unnecessary data that increases data security risks and costs of discovery in litigation. They also need to implement and document administrative, technical, and organizational data security measures (TOMs) that they require vendors to follow and to which they can commit contractually

vis-à-vis customers. Good TOMs also help protect trade secrets, comply with U.S. and other countries' data privacy laws, and reduce the risk of costly security breaches. But data security breaches will happen. It is not a question of "if," but "when" and "how prepared are you?" Given the excessively broad definitions of "personal data" and "personal data breach" in GDPR article 4(1) and (12), and a seventy-two-hour notification deadline in article 33, companies need to prepare well in advance on how to address security incidents, ideally with a dedicated response team, meaningful protocols for all employees, regular training, and repeated dry runs.

3. **Implement adequate data processing agreements.** Companies are required to sign contracts with their vendors and customers under various legal and industry-standard regimes that prescribe particular clauses and formats. In practice, businesses tend to err on the side of being over-inclusive with their vendors and include EU SCC 2010, clauses to be stipulated under GDPR article 28(3), HIPAA, PCI, and other regimes that may or may not apply to each and every vendor, but may come in handy as businesses evolve and downstream customers start formulating similar requirements. The standard contractual clauses that the EU Commission promulgated in 2010 for transfers to data processors outside the EEA are currently subject to legal challenges, but grandfathered under GDPR article 45(9) and also suitable for data transfers to processors within the EEA.[8] Your first priority action item is to sign up your vendors. If your company handles EU personal data for corporate customers, you should also prepare an adequate data processing agreement for your customers, to avoid a classification and obligations as a data controller under GDPR article 28(10), which would create insurmountable obstacles to business.
4. **Establish processes to grant data subject rights.** Consumers and privacy activists in the EEA are expected to launch a barrage of requests for access and copies of data, erasure, restrictions, objections, and data portability. Companies need to prepare protocols and ideally automated processes, possibly on a geographically differentiated basis, per country or region, given that not all data subjects around the world expect or have such rights.
5. **Prepare and keep up-to-date records of data processing activities.** Under GDPR article 30, businesses have to prepare data inventories with

certain prescribed information for each legal entity and field of activity (*e.g.*, HR, customer data, marketing). Companies that have invested in extensive "data maps" and various automated tools for their global group of affiliated companies may have a head start, but still need to create records that respond to the specific GDPR requirements for each of their entities to avoid providing data protection authorities, data subjects, works councils, or others with too much information.

6. **Document compliance with each applicable privacy principle and legal requirement in a dossier.** Companies are required to conduct, document, and potentially share with data protection authorities data protection impact assessments and "data protection by design" analyses. More broadly, companies are required to demonstrate how they comply under GDPR article 5(2). This necessitates extensive compliance documentation.
7. **Update your intercompany data transfer and processing compliance documentation.** The GDPR grandfathers existing European Commission decisions regarding countries' adequacy and standard contractual clauses, as well as authorizations by EU member states or supervisory authorities, but nevertheless generally requires updates to binding corporate rules, data processing agreements, consents, and other mechanisms.[9]
8. **Update data privacy notices.** Companies have to issue detailed information regarding their data processing practices relating to their websites (including "cookies"), mobile sites, customers, vendors, employees, job applicants, callers, marketing email recipients, and other data subjects. GDPR article 12(1) mandates "a concise, transparent, intelligible and easily accessible form, using clear and plain language." Yet, the additional requirements in articles 13 and 14 regarding notice content render this all but impossible, given the excessively prescriptive mandates for very complex and technical details, including a requirement to disclose "the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available."

9. **Appoint a local representative** for entities outside the EU per GDPR article 27. Companies outside the EEA can appoint one of their subsidiaries in the EEA, if any.
10. **Mind the ROW.** While you are comprehensively reviewing and upgrading your compliance program with respect to the GDPR, 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.[10]

What's Next?

On May 25, 2018, take a deep breath. And then—go back to work on May 26, 2018, because your company has to keep its data privacy law compliance program up to date. Your business and data processing practices are changing. Tomorrow, there will be new laws, guidance, cases, and customer demands regarding GDPR and other privacy laws.

Lothar Determann is a partner at Baker & McKenzie LLP, where his practice focuses on data privacy law compliance, information technology, copyrights, product regulations and international commercial law. Prof. Determann has been co-chairing PLI's annual program IP Issues in Business Transactions since 2008 and frequently speaks at other PLI programs, including TechLaw Institute 2018: The Digital Evolution and Eighteenth Annual Institute on Privacy and Data Security Law. He has authored more than 100 articles and five books on technology and data privacy–related topics, including *Determann's Field Guide to Data Privacy Law* (3d ed. 2017).

NOTES

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119), 1.
2. Commission Directive 95/46/EC, of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
3. Lothar Determann, *How to Ask for a Cookie: Information Technology, Data Privacy and Property Law Considerations*, 15 Electronic Com. & L. Rep. (BNA) 8 (Feb. 24, 2010).
4. Lothar Determann, *Less Than 20 Weeks to the European Union GDPR—What to Do Now?*, 17 Privacy & Sec. L. Rep. (BNA) 50 (Jan. 15, 2018).
5. Lothar Determann, *No One Owns Data* (Feb. 14, 2018) (Univ. Cal., Hastings, Research Paper No. 265), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3123957 (abstract).
6. *See* California Consumer Privacy Act, www.caprivacy.org (last visited Mar. 26, 2018).
7. *See* Lothar Determann, Determann's Field Guide to Data Privacy Law: International Corporate Compliance §§ 1.1–1.15 (3d ed. 2017).
8. *See* Lothar Determann, *EU Standard Contractual Clauses for Transfers of Personal Data to Processing Service Providers Reassessed*, 10 Privacy & Sec. L. Rep. (BNA) 498 (2011).
9. *See* Lothar Determann, Brian Hengesbaugh & Michaela Weigl, *The EU-U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options*, 15 Privacy & Sec. L. Rep. (BNA) 1726 (Sept. 5, 2016).
10. *See* Lothar Determann, California Privacy Law: Practical Guide and Commentary (Int'l Ass'n Privacy Prof'ls 3d ed. 2018).