Proskauer

European Union's General Data Protection Regulation (GDPR) To-Do List

Questions about GDPR? Contact:

Daniel Ornstein, Partner
+44.20.7280.2067
dornstein@proskauer.com

Kelly McMullon, Associate
+44.20.7280.2137
kmcmullon@proskauer.com

Stéphanie Martinier, Associate
+33.1.53.05.60.27
smartinier@proskauer.com

Mathilde Pepin, Associate
+33.1.53.05.60.10
mpepin@proskauer.com

1. Know what personal data you are processing. Personal data generally includes anything that can identify an individual. Data mapping should cover:
   - *a) Employee/customer/vendor data*
   - *b) Location of the data*
   - *c) How it's being used and with whom it's being shared*
   - *d) Identification of any "special categories" of personal data, such as data relating to race/ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sexual orientation and criminal history*

2. Determine whether the company is required to appoint a data protection officer. Either way, appoint an individual to be in charge of data privacy compliance within the company.

3. Decide how the company will receive and process requests from EU individuals to:
   - *a) receive a portable copy of the personal data that the company has about them,*
   - *b) make changes to the personal data that the company has about them,*
   - *c) opt out of automated decision making by the company, and*
   - *d) request that the company delete the personal data that it has about them*

4. Determine whether privacy impact assessments should be done. If so, create a template and process for performing them and for identifying new processes.

5. Update and/or prepare website privacy notice as well as privacy notices to employees, customers, clients and other data subjects about whom the company processes personal data.

6. Decide what your legal basis is for processing the data. In many cases, it will be for the purpose of performing under an agreement with the data subject, or for your own legitimate interests. To the extent that consent is being relied upon, review the method of obtaining that consent to see that it complies with the GDPR's requirements for consent.

7. Document the information security program and security incident response program.

8. Determine which member state the company desires to identify as its "one-stop shop" data protection authority. Determine whether registration requirements apply in that member state.

9. Inventory and prioritize third parties that process personal data on behalf of the company, like vendors and service providers. Check existing contracts to see whether GDPR-style provisions are included.

10. Determine how the company legitimizes exporting personal data from Europe under the existing Personal Data Directive. Model contracts? Privacy Shield? Binding corporate rules? Depending on what is already in place, determine how the company will legitimize exporting the data from Europe under the GDPR.

11. Review or prepare a record retention policy, determining how long personal data can be retained and under what circumstances it must be deleted or de-identified.

12. Check existing employee training modules to ensure that they cover what is required under GDPR.

13. Decide how the company will document its data processing activities now and going forward.