10 Things to Know About the GDPR

In May 2018, the EU General Data Protection Regulation (GDPR) will come into effect. The GDPR introduces a number of new requirements in the area of data privacy. Some of these requirements are onerous and companies therefore were given two years to adjust their practices. We are now half way through the transition period.

The GDPR focusses heavily on "accountability", meaning that companies must be in a position to demonstrate to regulators that they comply with the new rules. In addition, the GDPR significantly strengthens the enforcement environment by improving coordination among Supervisory Authorities ("SAs") and dramatically increasing the level of fines.

Here are ten top priorities that companies should consider as they prepare for the GDPR.

1. Territorial Scope

The GDPR applies to companies established in the Union, but also to companies that have no establishment in the Union, when they offer goods and services to individuals in the Union (i.e., targeting EU customers) or monitor the behavior of individuals in the Union (i.e., with tracking technologies). In this case, the companies must a appoint a representative in the Union.

2. Transparency

The GDPR expands the list of information that must be provided to individuals whose personal data is collected. For example, companies must now inform individuals about the data retention periods, the details on international transfers and related safeguards, and the right to lodge a complaint with a SA. Companies should start reviewing their privacy notices and policies to conform to the new GDPR transparency requirements.

3. Consent

An individual's consent is still a valid justification (legal basis) to process personal data. However, reliance of consent is now subject to additional requirements and restrictions. In particular, consent must be, unambiguous, specific and informed, and freely given. In an online context, unambiguous consent can be derived from the clicking of a box or tweaking privacy settings, but "silence, pre-ticked boxes or inactivity" does not constitute consent. In addition, the execution of a contract should not be conditioned on consent for data collection and processing that is not necessary for the performance of a contract. When included in a broader text, the consent language must be highlighted. The GDPR also contains specific rules on consent by children and, in the context of Internet services, imposes an age limitation of 16 years, which Member State can reduce to 13. Finally, individuals' right to withdraw consent must be as easy

to exercise as their ability to provide it. In light of the above, companies should assess whether they can or should continue to rely on consent or whether alternative justifications for their processing operations are more appropriate.

4. Register of Processing Operations and Privacy Impact Assessments

The GDPR requires companies with more than 250 employees to maintain a record of processing activities. There are specific format and content requirements and the register must be made available to the SA on request. The register is intended to replace the current time consuming notification the SA. In some cases, companies may also be required to implement Privacy Impact Assessments, for example, where they process sensitive data on a large scale.

5. Data Protection Officer (DPO)

The GDPR provides for the mandatory appointment of a DPO where the core activities of a company involve monitoring individuals or processing special categories of data on a large scale. EU or Member States may also provide for other situations where a DPO must be appointed. Companies should start assessing whether they have to appoint a DPO and, if so, make arrangement to do so. Given the potential headcount implications and the required decision-making time, the possible DPO requirement should be treated as a priority.

6. Security Breaches

Companies must notify data breaches to the competent SA “without undue delay” and, where feasible, no later than 72 hours after becoming aware of the breach, subject to exceptions. They must also communicate data breaches to the affected individuals if the breach is likely to result in a high risk, again subject to exceptions, such as appropriate encryption. The GDPR also sets out the content requirements of a breach notification. Companies should prepare or revise data breach response plans to make sure they can meet the imposed obligations as efficiently as possible.

7. Outsourcing

As under the current regime, the GDPR allows for the use of data processors (companies that process data on your behalf and under your instructions). However, the GDPR imposes more detailed obligations in respect of the minimum content of processor agreements. The GDPR also contains important conditions for the use of sub-processors. Companies should start reviewing their processing agreements and negotiate appropriate amendments with their service providers.

8. Rights

The GDPR focusses heavily on the rights of individuals. First, these rights are generally strengthened. For example, companies must facilitate the exercise of the rights within a set timeframe of one month and they may not charge a fee. Second, new rights have been introduced, such as the right to erasure (the so-called right to be forgotten”), the right to data portability and the right to restriction of processing. Companies should review their internal

procedures to make sure they can comply with the new requirements and can address requests from individuals.

9. International Transfers

The basic principles and restrictions in relation to international data transfers continue to apply. In a number of cases, the approval process has been simplified. Companies should continue to review their data flows, and, over time, consider alternative transfer mechanisms, such as Binding Corporate Rules, now that the adoption process has been simplified.

10. Training

Companies have a general obligation to implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance of data processing with the GDPR. This may include the implementation of appropriate data protection policies, but also the provision of privacy training to relevant staff involved in the processing of personal data.