

TEN STEPS TO DEAL WITH THE GDPR

Key Provisions and Practical Steps for Implementation

The EU General Data Protection Regulation (GDPR) was adopted in April 2016 and will enter into force in mid-2018. The GDPR, which is intended to create a single law on data protection across the EU, will have a significant impact on European companies and, importantly, also on businesses outside of Europe, such as in the U.S., that collect data on Europeans through offering goods or services to them or monitoring them. This is particularly important given the significant fines being introduced by the GDPR for non-compliance of up to 4% of annual worldwide turnover (gross revenue). Companies should now seriously consider the impact of the GDPR by carrying out an internal gap analysis of current data protection practices as compared to new requirements and rights under the GDPR. Below is a summary of some of the key provisions in the GDPR that need to be considered as part of the gap analysis together with some practical steps for implementation.

1

NOTICE AND CONSENT

Provide detailed information to individuals as required under GDPR and deal with new consent requirements (e.g., right of withdrawal at any time).

- ★ Review and amend existing employee and customer data privacy notices, consents and policies.
- ★ Review legal grounds for processing. If consent is needed, then determine how this will be obtained (i.e., opt-in and not implied).

2

DETAILED RECORDS

Under GDPR companies must maintain detailed records of data processing activities.

- ★ Carry out and maintain a data flow analysis to document the internal use of personal data by the business.

3

DATA PROTECTION OFFICER (DPO)

A DPO must be appointed under GDPR where: (i) processing large amounts of sensitive personal data (e.g., health data); (ii) regularly monitoring individuals; or (iii) required by Member State law.

- ★ Determine if a DPO is required, and if so, whether to appoint a single DPO (with privacy representatives in each local entity) OR a DPO for each business unit; and decide if DPO will be an employee or engaged as a service provider.

4

PRIVACY IMPACT ASSESSMENTS (PIAs)

Under GDPR PIAs must be completed where using new technologies and processing is likely to result in a high risk to individuals (e.g. profiling or the use of health data on a large scale).

- ★ Develop a process to ensure PIAs are carried out when necessary and reviewed when risks change.
- ★ Consider developing a template PIA for use by the business.

5

PRIVACY BY DESIGN AND BY DEFAULT

Implemented technical/organizational measures to ensure GDPR requirements (privacy by design) are met AND only the minimum amount of data are processed by default.

- ★ Review IT systems and document retention procedures to assess impact of GDPR privacy by design and data minimization requirements.

6

REPORTING SECURITY BREACHES

Under GDPR personal data breaches must be reported without undue delay to the Data Protection Authority and where feasible within 72 hours. Where the breach is likely to result in a high risk to affected individuals (e.g., customers), they must be notified without undue delay unless measures taken to minimize risk (e.g., encryption).

- ★ Review and update information security standards and policies and implement a process for regular security audits.
- ★ Develop a response plan to ensure data breaches are detected, reported and investigated efficiently and effectively.

7

DATA PROCESSORS

For the first time, GDPR imposes statutory requirements/liabilities for processors (e.g., vendors).

- ★ Review vendor agreements to verify provisions for liability and security breach reporting.
- ★ Consider implementing a management program consisting of a vendor questionnaire, minimum security requirements and regular vendor audits.

8

NEW DATA SUBJECT RIGHTS

Under the GDPR there are new rights to: (i) erasure (e.g., when data is no longer necessary or consent is withdrawn); (ii) object to processing, including in relation to direct marketing; and (iii) data portability (i.e., transferring data to another controller where processing is based on consent or on the performance of a contract).

- ★ Assess impact of new data protection rights on the business.
- ★ Develop policies, procedures and system changes based on the impact of these new rights on the business.

9

PROFILING

The GDPR imposes new restrictions on businesses that conduct profiling with some exceptions, such as where: (i) necessary for the performance of a contract; (ii) authorized by Member State law; or (iii) conducted with the individual's explicit consent.

- ★ Review consents and notices and determine whether current profiling activities are covered by an exception.
- ★ Amend profiling activities as necessary to ensure compliance with the GDPR.

10

INTERNATIONAL DATA TRANSFERS

GDPR maintains restrictions on transfers of personal data to countries outside the EEA that are deemed by the EU to not provide an adequate level of protection. International transfer solutions include: (i) EU Standard Contractual Clauses; (ii) Binding Corporate Rules; (iii) approved Codes of Conduct or certification mechanisms; and (iv) EU-U.S. Privacy Shield (if adopted).

- ★ Determine international data flows based on review of processing activities.
- ★ Consider international transfer solutions in light of recent developments on EU-U.S. Privacy Shield and other solutions and implement appropriate solutions.



SIDLEY

AMERICA • ASIA PACIFIC • EUROPE

sidley.com