9 QUESTIONS TO ASK YOURSELF WHEN PREPARING FOR THE GDPR

PROJECT MOORE

WHY? STRICTER RULES, HIGHER FINES

The General Data Protection Regulation will enter into effect in May 2018. Because it will entail serious new obligations, near-global jurisdiction, and penalties of up to 4% of worldwide annual turnover, now is the time to ask yourself these nine questions.

GOVERNANCE LEVEL

1 Have you set up your project team?

The stakes will be higher and accountability requirements stricter. Smart governance structures, clear responsibilities, and focused policies for handling and retaining data will enable you to take action and mitigate risks. Your company's experts in legal, compliance, IT, security, and HR all need to be made aware of and become involved in these aspects, for example, through a dedicated project team.

2 Do you need a data protection officer?

Specific data processing operations, such as high-risk analytics, trigger an obligation to appoint a data protection officer. A strong DPO with the role and position to independently advise on compliance and report to the board is essential for these kinds of organisations.

3 Is your record keeping up-to-date?

Not only must organisations comply, they must demonstrate their compliance. This means carrying out privacy-impact assessments, especially for high-risk operations, documenting decisions, and keeping records of all data processing activities. Clear organisational processes and carefully crafted data management frameworks provide a sturdy foundation.

DESIGN LEVEL

4 Is your IT-design privacy-friendly?

Organisations need to incorporate data protection principles into their technical systems (privacy by design). And they must make sure that default settings keep processing to a minimum (privacy by default). Involving developers, designers, and data protection experts throughout the production process leads to compliant products and services.

5 Are you prepared for a data breach?

Organisations will be required to report data breaches. You must be able to detect, investigate, and report data breaches as soon as they occur. A security incident response plan and clear procedures will help a dedicated data breach team act swiftly when this happens.

6 Can you handle data subject requests?

Existing individual rights will be enhanced and new rights, such as the right to data portability, will be introduced. A systematic schedule and overview of data processing within your organisation will allow you to be fully prepared when individuals exercise their rights. The mere addition of a privacy dashboard might save you a great deal of hassle, allowing users to view, edit, and export their data.

EXECUTION LEVEL

7 Have you updated your privacy notices?

Organisations need to provide individuals more information about what they do with personal data, including their retention terms, processing reasons, and profiling considerations. Effective, understandable, and well-designed privacy policies, app notifications, and other customer-oriented materials lead to better-informed individuals.

8 Do you use cutting-edge consent forms?

It will become more difficult to obtain valid consent, especially for sensitive data and data involving children. Clear, tailor-made online forms, consent boxes, and app confirmations will be necessary to ensure that consent remains valid in the future.

9 Are your contracts future-proof?

More contractual obligations will be required between controllers and processors. A quick scan of existing vendor agreements to ensure compliance will give you peace of mind. And well-drafted standard purchase conditions can minimise liability in the future.

PROJECT MOORE, AN AMSTERDAM LAW FIRM SPECIALISING IN IT LAW AND PRIVACY

CALL US. +31 20 5200 870

or visit https://projectmoore.com