KING & SPALDING

General Data Protection Regulation (GDPR) Compliance Test

Companies processing "personal data" and operating in the EU must comply with the General Data Protection Regulation (GDPR). Has your company taken all the steps required to comply?

Has your organization focused on the definition of personal data under GDPR?	GDPR protects the personal data of individuals in the EU. The GDPR definition of "personal data" is much broader than the definition of "personally identifying information" (PII) in the U.S. It includes names, email addresses, postal addresses, on-line identifiers, and any other data that identifies a living person, alone or in combination with other data about the individual.
Do you know your personal data?	Do you understand the personal data you collect, how it is used, where it is stored, and whether it is properly secured for its level of sensitivity? Do you know who has access to it and how and where it is transferred and processed? You must know these answers to be able to comply.
Is data protection part of your organization's DNA?	GDPR mandates that you apply the principles of data protection by design and by default, meaning you must design and maintain systems and processes to protect data. Examples include adopting techniques such as encrypting data to avoid unauthorized access, conducting data protection risk assessments, and data minimization.
Are your documents GDPR compliant?	Privacy notices, privacy policies, contracts of employment, staff handbooks, and data retention policies should be reviewed and updated to address GDPR standards. Additionally, policies must be implemented in practice by the organization.
Do you have an incident response plan?	GDPR imposes data breach notification rules on organizations for the first time. Data controllers must report breaches to regulators within 72 hours of becoming aware and potentially notify customers. To comply, your company must have a plan for handling data breaches.
Have you reviewed third-party contracts?	Anyone processing the personal data you hold, from a cloud service provider to a benefit provider, must meet an appropriate data protection maturity level. In addition to written requirements for data processing agreements, processors must (1) ensure data protection by design and default and (2) implement technical and organizational measures for data integrity and confidentiality.
What legal basis do you rely on to justify processing?	It will no longer be enough to infer consent from silence, pre-ticked boxes or inactivity. You will need to review how consent is obtained and consider whether any changes need to be made, or whether existing consents need to be renewed. Individuals must be able to withdraw consent as easily as it was given, and your procedures must reflect this.

WHEN DOES GDPR APPLY?

- ✓ When a business has operations in the EU or is doing business in the EU that processes personal data
- ✓ When a U.S. business is targeting or offering goods and services to consumers in the EU

94% of U.S. firms possess EU customer data, but only 58% have a "detailed and far reaching plan" to comply with GDPR according to a recent Compuware report.

FOR MORE INFORMATION, CONTACT:

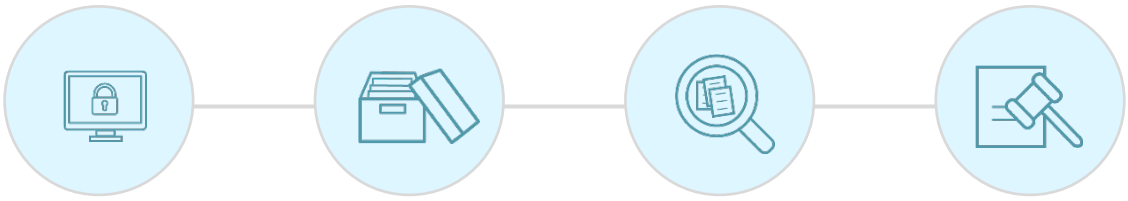
Phyllis Sumner
Partner, Chief Privacy Officer
+1 404 572 4799
psumner@kslaw.com

Kim Roberts
Counsel
+44 20 7551 2133
kroberts@kslaw.com

To view or contact our team, please visit kslaw.com.

May 25th has come and gone – What happens next?

What are the most serious threats following the implementation of GDPR, and what is on the horizon?



The vastly expanded set of powerful rights that individuals have in relation to their personal data is a significant concern. Many corporations are still struggling with the operationalization of these rights. Our clients report that they are experiencing extensive challenges with locating the entirety of the data that they hold on an individual in response to a request, and difficulty managing requests within the statutory time period. Some industries are particularly affected and are receiving hundreds of data subject access requests from single claims handlers, which are extremely difficult and time consuming to manage.

Immediately following the implementation of GDPR, activist-led campaigns were launched in France against major tech giants, brought by groups made up of thousands of complainants relating to the issue of whether sufficiently specific consent for use of personal information has been obtained by tech companies. These campaigns have gathered significant media attention, but have not yet been determined by the French regulator.

In terms of regulator led action, there are, as of yet, no obvious enforcement trends to observe under GDPR, with minimal court rulings available. We are regularly asked why regulators have not moved more quickly to use their powers to issue hefty fines to corporations which are non-compliant with GDPR. The answer seems to be simple: it takes time to prepare a complaint, wait for a response from the defaulting company, evaluate that response, seek further evidence, etc. There is also a perception that the regulators are concerned that they get the first big hit right, remembering that they are perhaps not as “lawyered up” as the large global corporations, which are more seasoned in defending their corporate positions.

The regulators have, however, not missed the opportunity to communicate the wide range of enforcement powers that GDPR allows. In addition to the fines, GDPR provides investigative powers, such as to order provision of information or to carry out audits, and corrective powers, such as to issue warnings and “cease processing” notices, a potentially devastating outcome for a non-compliant corporation.

Data breach reports have increased enormously since GDPR came into effect, and the UK regulator, the ICO has reported that it now receives around 500 calls each week to its data breach hotline. While underreporting of data breaches before GDPR came into effect was a concern, this spike suggests overreporting is taking place, and that corporations do not want to make a mistake regarding the new and onerous reporting requirements. The ICO plans to issue new guidelines on when a data breach must be reported to address this issue.

A Trust Arc report tells us that as of July 2018 only 11% of US companies considered themselves compliant with GDPR on the effective date of May 25, 2018, with 20% still working on their preliminary GDPR plan and 22% still working to implement the plan. Without a doubt, the threats are manifold and compliance with GDPR must remain a key focus for companies and an ongoing requirement.