LOCKE LORD® QUICKStudy
Privacy & Cybersecurity Practice
February 14, 2018

GDPR – 100 Days to the Great Data Protection Revolution

By: Andrew Shindler and Thomas J. Smedinghoff

In 100 days, on 25 May 2018, the EU's new data protection law goes live. The General Data Protection Regulation, commonly known as the GDPR, is the biggest change to European data protection law in over 20 years and will seriously impact businesses across the USA and around the world.

With only 100 days to go, time is running out for pro-active compliance activity.

In this *QuickStudy*, we highlight some of the most far-reaching changes and burdensome requirements.

Worldwide Application

The first thing for non-EU business to consider is whether they are subject to the GDPR: this new law may apply even if you don't have a legal or physical presence in the EU.

Now you will have to comply if you offer goods or services to individuals in the EU or monitor their behaviour on the internet. A recent international report found that more than 70% of non-EU respondents said the GDPR would apply to their organisations.

Over recent months., Locke Lord has advised numerous US and internationally-headquartered clients on whether the GDPR applies to their businesses.

Fines and Other Sanctions

The maximum fine for breaching the GDPR is up to 40 times larger than under the previous law, and even more for big business - EU data authorities have been given the power to levy fines up to €20 million or 4% of the annual worldwide gross revenue of the whole group, whichever is greater.

That said, fines must be proportionate and are discretionary and applied on a case by case basis.

However, fines are only part of the story: in cases of breach; adversely affected individuals can claim compensation and breaches frequently result in negative publicity which can have a severe financial impact which in extreme cases can destroy a business.

Enhanced Rights of Data Subjects

Individuals have a right to obtain copies of all their personal data you are processing, generally within 30 days. They also have the right to have it ported to another provider or to object to its processing on certain grounds. They may also be able to require its erasure – the "right to be forgotten".

Reporting Data Breaches

There is a legal obligation to report a personal data breach to the authorities without undue delay - generally within 72 hours. This includes instances of hacking or where you have lost personal data you were holding, wherever there is a risk to individuals.

In serious cases, all the individuals potentially affected by the data breach must also be notified, unless the data accessed is properly protected, e.g. by encryption.

Information Notices

You must provide individuals with extensive information about how you will process their data – in a transparent, intelligible and easily accessible way, using clear language.

Higher Standard for Consent

If you rely on "consent" for processing personal data – the GDPR has raised the bar. Separate consents are now required for different processing activities. Pre-ticked boxes and blanket consents are not valid and individuals must be able to easily withdraw consent at any time.

For children under 13, and potentially up to 15, consent from a parent is required.

Processors Now Liable

Under the previous law, where a business processed personal data strictly on someone else's instructions, it was a data "processor" rather than a data "controller" and not directly subject to EU data protection law. This is no longer the case; data processors have many of the same obligations as data controllers and both are jointly liable for breaches they are involved in.

Data Protection Officers - "DPOs"

Public authorities, organisations whose core activities require regular and systematic monitoring of data subjects on a large scale, or which process special categories of data on a large scale, **must** appoint a DPO. Other organisations which process significant personal data are recommended to make such an appointment.

The DPO must carry out a variety of data protection advisory, monitoring and other functions. He/she must be suitably skilled and experienced, properly resourced and report to the highest levels of management without receiving any instructions and without conflict of interest.

A recent international study found that in Europe alone, 28,000 DPOs will need to be appointed by 25 May 2018.

Privacy Impact Assessments

If you are engaged in "high" risk processing - processing that presents a risk of infringing a person's rights and freedoms, such as large scale processing of sensitive data or monitoring and profiling individual activities – you must carry out a Privacy Impact Assessment or "PIA". This is a thorough exercise and organisations are likely to require guidance on how to undertake it.

Cybersecurity

Organisations must have appropriate security measures in place to protect personal data. In particular this requires technical cybersecurity, such as ISO 27001 certification, but also includes organisational policies and staff training.

Keep Calm but Act Now

With 100 days to go, now is the time for action – if unsure what to do or whether the GDPR applies to your business please get in touch with one of our key contacts.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact the authors.

Andrew Shindler | +44 (0) 20 7861 9077 | andrew.shindler@lockelord.com
Thomas J. Smedinghoff | 312-201-2021 | tom.smedinghoff@lockelord.com