The General Data Protection Regulation (GDPR) promises the biggest shake up to European privacy laws for 20 years. It will apply in all European Member States from 25 May 2018.

The GDPR will not only bring a step change in sanctions, with fines of up to 4% of annual worldwide turnover or €20 million, but will also change the way your customers and others expect you to handle their personal information.

Businesses based in the UK should continue to prepare for the GDPR, notwithstanding Brexit. It is likely that the rules in the GDPR will still be applied to the UK for the short to medium term. Moreover, if your business deals with individuals in the rest of EU, you will be caught by the extra-territorial provisions in the GDPR. Similarly, if parts of your business are established in the rest of the EU, those establishments will be directly subject to the GDPR.

This leaflet summarises the key changes under the GDPR, as well as offering a “to do” list to help you prepare for 2018. The changes needed to comply with the GDPR are significant, and you should start to prepare for them now.

We have also produced a Survival Guide on the GDPR which considers all of these issues in much greater detail.

The Survival Guide is available at www.linklaters.com/GDPR.

Tanguy Van Overstraeten
Global Head of Data Protection
Tel: (+32) 2 501 94 05
tanguy.van_overstraeten@linklaters.com

Richard Cumbley
Global Head of TMT/IP
Tel: (+44) 20 7456 4681
richard.cumbley@linklaters.com

Daniel Pauly
Partner
Tel: (+49) 69 710 03 570
daniel.pauly@linklaters.com

The purpose of this leaflet is not to provide legal advice or exhaustive information but rather to create awareness of the main rules under the General Data Protection Regulation. If you have any questions about the issues raised or if specific advice is needed, please consult one of the lawyers referred to in the contact list at the end of this leaflet.
At a glance: what you need to know, what you need to do

The GDPR will apply from 25 May 2018.

The GDPR retains the same core rules as the existing Data Protection Directive but there are some significant changes to those rules.

The concept of sensitive personal data has been retained and expanded to include genetic and biometric data. Using information about criminal offences will also be harder to justify.

There are also potentially significant new rights for individuals, including the “right to be forgotten” and the right to data portability.

The new rights are complex and it is not clear how they will operate in practice.

Under the GDPR, you must not only comply but also be able to demonstrate you comply.

If you are carrying out “high risk” processing, you must carry out a privacy impact assessment and, in some cases, consult your regulator. This could have significant timing implications for your project.

You may be obliged to appoint a data protection officer. The data protection officer must be involved in all data protection issues and must report directly to the highest level of management within your organisation.

You may keep personal data secure. This obligation is expressed in general terms but does indicate that some nuanced measures, such as encryption, may be needed.

You may have to report security breaches to the regulator and, in some cases, to individuals.

You will need to include new obligations in contracts with your data processors.

Some aspects of the GDPR are directly applicable to processors. This will be a major change for some suppliers who were previously not subject to data protection law.

The GDPR prohibits the transfer of personal data outside the EU, unless certain conditions are met. These conditions are broadly the same as those under the existing Data Protection Directive.

Full compliance with these rules will continue to be difficult and requests from foreign regulators will be challenging.

Work out where your main establishment is and who your lead regulator will be.

Evaluate if your business (if established outside the EU) is nonetheless caught by the GDPR. If you are caught, you may need to appoint an EU representative.

Consider if you want to take steps to avoid being subject to the GDPR.

Review your existing processes to obtain consent if they are processing genetic or biometric information or information about criminal offences. If so, bring that processing into line with the new requirements of the GDPR.

Consider if individuals are likely to exercise their new rights against you and what they mean for your business in practice.

Consider that you can rely on an alternative basis for processing, especially in light of the right to withdraw consent.

You will need to create and maintain a record of the processing you are carrying out (unless exempt).

You should adopt your product development processes to include a privacy impact assessment.

You will have to update your existing privacy notices.

Work out if you need to appoint a data protection officer or want to appoint one on a voluntary basis.

Consider if you want to appoint a central breach management unit to collate, review and notify breaches, where appropriate.

Review and update your security measures in light of the increased security obligations in the GDPR.

Consider setting up a central breach management unit to collate, review and notify breaches, where appropriate.

If you are a controller, update your contracts with processors to reflect the new contract requirements.

If you are a processor, consider implementing a “structured” transfer solution (such as binding corporate rules or an intragroup agreement) to justify your transfers.

Review your current transfers and consider if they are justified now and will continue to be justified under the GDPR.

You should consider implementing a “structured” transfer solution (such as binding corporate rules or an intragroup agreement) to justify your transfers.

Further information on all these issues is available in our Survival Guide www.linklaters.com/GDPR
Contacts

Brussels
Tanguy Van Overstraeten
Tel: (+32) 2 501 94 05
tanguy.van_overstraeten@linklaters.com

Frankfurt
Daniel Pauly
Tel: (+49) 69 710 03 570
daniel.pauly@linklaters.com

Hong Kong
Samantha Cornelius
Tel: (+852) 2901 5542
samantha.cornelius@linklaters.com

Lisbon
Carlos Pinto Correia
Tel: (+351) 21 864 00 15 5015
carlos.correia@linklaters.com

London
Richard Cumbley
Tel: (+44) 20 7456 4681
richard.cumbley@linklaters.com

Luxembourg
Olivier Reisch
Tel: (+352) 2608 8294
olivier.reisch@linklaters.com

Madrid
Carmen Burgos
Tel: (+34) 91 399 6088
carmen.burgos@linklaters.com

Moscow
Evgeny Ulumdzhiyev
Tel: (+7) 495 797 9797
evgeny.ulumdzhiyev@linklaters.com

Munich
Konrad Berger
Tel: (+49) 89 418 08 168
konrad.berger@linklaters.com

Paris
Sonia Cissé
Tel: (+33) 1 56 43 57 29
sonia.cisse@linklaters.com

Singapore
Adrian Fisher
Tel: (+65) 6692 5856
adrian.fisher@linklaters.com

Stockholm
Elisabet Lundgren
Tel: (+46) 8 665 67 77
elisabet.lundgren@linklaters.com

Tokyo
Mamiko Nagai
Tel: (+81) 3 6212 1232
mamiko.nagai@linklaters.com

Warsaw
Piotr Zawadzki
Tel: (+48) 22 526 5045
piotr.zawadzki@linklaters.com

linklaters.com

A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ, England or on www.linklaters.com and such persons are either solicitors, registered foreign lawyers or European lawyers. Please refer to www.linklaters.com/regulation for important information on our regulatory position.