The General Data Protection Regulation 2016 (GDPR) will apply across the EU from 25 May 2018. The UK government has confirmed that this includes the UK. The GDPR is a complete overhaul of EU data protection law and, given the exponential growth in the use of personal data by organisations, is hugely significant, affecting the widest range of organisations.

GDPR – the headlines
The GDPR introduces new rights for individuals and places an enhanced compliance burden on organisations together with potential fines up to the higher of 4% of annual global turnover or 20m Euros for non-compliance.

Key points to note are:

- **Territorial scope** – expansion of territorial scope to include applicability to non-EU organisations offering goods or services to data subjects in the EU or monitoring their behaviour to the extent that the behaviour takes place in the EU.

- **Notification** – no requirement to notify authorities of data processing but a requirement to keep records of data processing activities (subject to limited exceptions for SMEs).

- **One Stop Shop** – organisations will be regulated by a single ‘lead’ regulator in the place of their main establishment. The main establishment will be the main administrative location in the EU unless the main decisions about data processing are taken in a different Member State in which case that will be the main establishment. Individuals will be able to make complaints in their Member State at which point that regulator will engage in a cooperation procedure which will be settled by the European Data Protection Board in the event of disagreement. Member State regulators will also be able to deal with any issues arising in their own jurisdictions subject to a cooperation procedure.

- **Penalties** – maximum penalties of 4% annual global turnover or up to 20m Euros (whichever is higher).

- **DPOs** – requirement to appoint a data protection officer (DPO) where an organisation’s core business involves processing personal data involving regular and systematic monitoring of data subjects or large amounts of sensitive personal data. Member States will have discretion to enact national provisions imposing further requirements regarding the appointment of DPOs.
Breach reporting – breaches must be reported to the relevant regulator without undue delay and, where feasible, within 72 hours of becoming aware of it unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Data subjects must be informed without undue delay where the breach is likely to result in a high risk to the data subject’s rights and freedoms unless the data has been rendered unintelligible to any third party (for example by encryption), the data controller has taken steps to ensure the high risk is unlikely to materialise or it would involve disproportionate effort to inform data subjects individually in which case a public announcement can be made. Data processors are required to inform data controllers of any breach without undue delay.

Consent – organisations relying on consent to process personal data will need to show that the consent is freely given, specific and informed and is an “unambiguous indication” of a data subject’s wishes and expressed either by a statement or a clear affirmative action. Consent will be purpose limited i.e. related to explicitly specified purposes.

PIAs – organisations will be required to carry out data protection impact assessments (PIAs) if their proposed activities are likely to result in a high risk for the rights and freedoms of individuals, in particular, through the use of new technologies and in cases of people profiling. If the PIA reveals a significant risk, the organisation must consult with their regulator before beginning the processing.

Data subject rights – new rights around data portability, the right to be forgotten and to prevent profiling. Continuation of right to object to processing, to rectification and erasure.

Privacy by design and default – enshrined into statute – controllers are specifically prevented from setting defaults to disclose data to all.

Purpose limitation – data processing must be carried out for the original purpose(s) for which it was collected unless the new purpose is a compatible one.

Data export to third countries – similar restrictions on transfers of personal data outside the EU as under current law. Data can be transferred under a Commission adequacy decision (the GDPR contains details of how these should be reached); standard contractual clauses or BCRs for intra-group transfers. In addition, there are limited possibilities to transfer data with consent or where it is necessary for the performance of a contract.

Data processors – parts of the GDPR will apply directly to data processors who will be subject to compliance requirements and to sanctions for non-compliance for the first time.

Digital consent for minors – while the default age for giving valid consent and using online services is set at 16, Member States will be able to reduce this to as low as 13.
GDPR – data privacy compliance programme

Under the GDPR, you not only have to comply with the law, you have to be able to demonstrate compliance under the accountability principle. The creation of a GDPR data privacy compliance programme is the first step.

▶ Who is responsible for personal data? – it is essential to have a data privacy governance structure in place. Whether or not you already have a DPO and whether or not you are required to appoint one under the GDPR, you need to identify the chain of responsibility and reporting lines around your use of personal data. It is essential for senior management to be involved from the outset and for data protection to be an issue which is scrutinised at board level. If you are going to have to appoint a DPO, start recruiting (either internally or externally) as soon as possible.

▶ Map your data – half the battle is understanding what personal data you control or process and what you do with that data. A formal data mapping exercise which documents this will not only help you understand what you need to do to be compliant under the GDPR, it will crucially also help you demonstrate compliance.

▶ Assess current practices – how compliant are you under current data protection law? Identify compliance gaps between current practices and future requirements.

▶ Review your privacy policies and terms and conditions – are these still going to be compliant? The GDPR requires transparency and has certain prescribed elements which must be included in privacy policies like, for example, informing data subjects of their rights under the GDPR.

▶ Review internal policies and train your staff – are your internal policies compliant? Do staff know what is expected of them with regard to processing personal data including dealing with data breaches, handling subject access requests and conducting privacy impact assessments?

▶ Review any data processor agreements – whether you are a controller or processor, you should look at existing and future agreements to ensure they adequately deal with responsibility and liability given the new direct compliance requirements for data processors.

▶ Look again at consent – it will be harder to meet consent requirements under the GDPR than under current law. If you rely on consent to process personal data, you will need to ensure it will still be valid. You may have to collect renewed consent and you must ensure consent is documented. You may also want to consider other purposes as a justification for processing the data, particularly in relation to HR data where valid consent will be very hard to achieve.

▶ Do you have adequate data security measures in place? – the GDPR requires both data controllers and processors to implement adequate technical and organisational measures to ensure data is processed securely and is adequately protected. You should be thinking about privacy by design and default, technical security measures and using techniques like pseudonymisation to minimise risk. It is not enough to do this once. You will need to ensure a rolling review and update system is in place.

▶ When will you need Data Protection Impact Assessments? – PIAs are a key tool under the GDPR for determining risk and, again, for demonstrating compliance for both data controllers and data processors. Ensure there is a policy for when and how PIAs need to be carried out and decisions made.

▶ Do you know how to handle a data breach? – even the most careful businesses are vulnerable to data breaches but their impact can be significantly minimised if you have a data breach plan in place. This will include knowing who your key contacts are, being able to minimise the risk to individuals, understanding when you need to report a data breach to your regulator or to affected data subjects, and the ability to identify the source of the breach and do what you can to make sure it doesn’t happen again.

▶ Are you exporting personal data outside the EEA? – while the rules around data exports are not changing dramatically, this is a good opportunity to review the legitimacy of data exports. This is all the more relevant as there are still question marks over export solutions to the USA. As Brexit approaches and the question of EU-UK data transfers becomes more significant, this is an area to watch closely.

▶ Know your regulator – one of the benefits of the GDPR is a simplified regulatory regime. Most organisations will be able to take advantage of the ‘one stop shop’ and deal mainly with a Lead Supervisory Authority. Identify your Lead SA (if you have one); they may be helpful in dealing with any compliance questions you have. The UK’s ICO certainly encourages consultation and is likely to be understanding of businesses doing their best to comply.
Find out more

We have a wealth of articles on our Global Data Hub. You can also access our data protection webinars from the Global Data Hub. If you would like to be kept up to date with the latest data protection materials, including weekly news, speak to your usual contact at Taylor Wessing or to a member of the core privacy team.

About Taylor Wessing

Taylor Wessing is a full-service international law firm, working with clients in the world’s most dynamic industries. We take a single-minded approach to advising our clients, helping them succeed by thinking innovatively about their business issues. Our focus on the industries of tomorrow has enabled us to develop market-leading expertise in:

- Private Wealth
- Life Sciences
- Energy
- Technology, Media and Communications.

At Taylor Wessing we are proud of our reputation as a forward-thinking firm. We support clients wherever they want to do business. Our 33 offices around the world blend the best of local commercial, industry and cultural knowledge with international experience to provide proactive, integrated solutions for our clients.