KEYSTONE LAW

GETTING AHEAD OF THE GDPR

The General Data Protection Regulation will come into force on 25 May 2018 and compliance will require significant investment. Getting it right will involve prioritisation, corporate culture and risk-tolerance assessments. Below is a comprehensive checklist demonstrating how you can get ahead of the curve.

Key concepts and changes	Impact	What businesses should be doing now
Greater harmonisation. The GDPR introduces a single legal framework that applies across all EU member states. This means that businesses will face **a more consistent set of data protection compliance** obligations from one EU member state to the next.	Positive	Greater harmonisation is broadly likely to be a positive change. However, the GDPR is still likely to require significant changes for many businesses, and many of these changes will require substantial lead time. It is therefore important for businesses to plan ahead.
Increased enforcement powers. The GDPR will significantly increase the maximum fines, and NDPAs will be able to impose fines on data controllers and data processors on a two-tier basis. The investigative powers of NDPAs include a power to carry out audits, as well as to require information to be provided, and to obtain access to premises.	Negative	Businesses that had previously regarded non-compliance with EU data protection law as a low-risk issue will be forced to re-evaluate their positions in the light of the substantial new fines, increased NDPA enforcement powers, and grounds for seeking judicial remedies under the GDPR.
Consent, as a legal basis for processing, will be harder to obtain. The GDPR requires a very high standard of consent, which must be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written (including electronic or oral) statement. An individual's explicit consent is still required to process special categories of personal data. Businesses must be able to demonstrate that the data subject gave their consent to the processing and they will bear the burden of proof that consent was validly obtained. The data subject shall have the right to withdraw their consent at any time.	Negative	Businesses in the UK have often tried to rely upon implied consent. Businesses that may have relied upon implied consent, as a legal basis for processing personal data, will need to carefully review their existing practices to ensure that any consent they obtain indicates affirmative agreement from the data subject (for example, ticking a blank box). Mere acquiescence (for example, failing to un-tick a pre-ticked box) does not constitute valid consent under the GDPR. Businesses must also consider how they will discharge the evidential burden of demonstrating that consent has been obtained. Businesses must ensure that an individual can withdraw their consent at any time. Changes to consent mechanisms will require careful review, and may take time to implement.

The risk-based approach to compliance. The GDPR adopts a risk-based approach to compliance, under which businesses bear responsibility for assessing the degree of risk that their processing activities pose to data subjects. This can be seen in several of the provisions – for example, the new accountability principle and requirement for data controllers to maintain documentation, privacy by design and default, privacy impact assessments, data security requirements and the appointment of a data protection officer in certain circumstances. Low-risk processing activities may face a reduced compliance burden.	Positive	As this may involve substantial changes to existing compliance strategies and arrangements, businesses should start their preparation now. Businesses should: • Create awareness among the senior decision makers in the business. • Audit and document the personal data they hold, recording where it came from and who it is shared with. • Review the legal basis for the various types of processing that they carry out and document this. • Review privacy notices and put in place a plan for making any changes to comply with the GDPR.
The "one-stop shop". Under the GDPR, a business will be able to deal with a single NDPA as its **"lead supervisory authority"** across the EU. Where a controller or processor has more than one establishment in the EU, the GDPR anticipates that they will have a main establishment and work with the NDPA for the main establishment where cross-border processing is involved. **("lead SA").** The lead SA will be responsible for all regulation of cross-border processing activities carried out by that controller or processor.	Positive	For businesses that only operate within a single EU member state, and only process the personal data of data subjects residing in that member state, interaction with the local NDPA under the GDPR will be similar to interaction with the local NDPA under the Data Protection Directive. Multi-nationals and businesses that operate in more than one EU member state will see a substantial change.
Privacy by design and by default, privacy impact assessments, prior consultation and standardised icons. **Mandatory privacy by design and default.** Having regard to the state of the art and the cost of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk to individuals, businesses will be required to implement data protection **by design** (for example, when creating new products, services or other data processing activities) and **by default** (for example, data minimisation) at the time of the determination of the means for processing and at the time of the processing itself.	Negative	In particular, the GDPR will require businesses to implement technical and organisational measures (such as pseudonymisation) to ensure that the requirements of the GDPR are met. Businesses must both: • Take data protection requirements into account from the inception of any new technology, product or service that involves the processing of personal data, with an ongoing requirement to keep those measures up to date. • Conduct data protection impact assessments (PIAs) where appropriate.
Mandatory privacy impact assessments. Businesses will be required to perform PIAs before any processing that uses new technologies (and taking into account the nature, scope, context and purposes of the processing) that is likely to result in a high risk to data subjects, takes place. In particular, PIAs will be required for: • A systematic and extensive evaluation of personal aspects by automated processing, including profiling, and on which decisions are based that produce legal effects concerning the data subject or significantly affect the data subject.	Negative	These steps will need to be planned into future product cycles. The Information Commissioner's Privacy Impact Assessments code of practice provides helpful guidance on when and how to implement PIAs.

• Processing of special categories of personal data or data relating to criminal convictions and offences on a large scale. • A systematic monitoring of a publicly accessible area on a large scale. The NDPA will publish a list of the kind of processing operations that require a PIA. **Mandatory prior consultation.** In addition, where a PIA indicates that the processing would result in a high risk to individuals, the business must consult, before any processing taking place, with the NDPA.	Negative	As per the a
Registrations. Instead of registering with an NDPA, the GDPR will require businesses to **maintain detailed documentation** recording their processing activities, and the GDPR specifies the information this record must contain. Data processors must keep a record of the categories of processing activities they carry out on behalf of a controller. The GDPR specifies what this record must contain. These obligations do not apply to an organisation employing fewer than 250 people unless the processing is likely to result in high risk to individuals, In addition, in certain circumstances, controllers or processors are required to **appoint a data protection officer.**	Little change	Businesses should: • Review their existing compliance programmes, and ensure that those programmes are updated and expanded as necessary to comply with the GDPR. • Ensure that they have clear records of all of their data processing activities, and that such records are available to be provided to NDPAs on request. • Appoint a data protection officer (particularly, where it is mandatory to do so) with expert knowledge of data protection.
New obligations of data processors. The GDPR introduces direct compliance obligations for processors. Under the GDPR, processors may be liable to pay fines of up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros, whichever is greater and as set out in the GDPR.	Negative	The GDPR is likely to substantially impact both processors and controllers that engage processors, in the following ways: • The increased compliance obligations. • Negotiating data processing agreements may become more difficult. • Some processors may wish to review their existing data processing agreements. • Data controllers should identify their processor agreements early on.
Strict data breach notification rules. The GDPR requires businesses to notify the NDPA of all data breaches (other than insignificant ones) without undue delay and where feasible **within 72 hours.**	Negative	Businesses will need to develop and implement a data breach response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling them to react promptly in the event of a data breach. Complying with the data-breach reporting obligations in the GDPR will also entail a significant administrative burden for businesses, which may increase costs.

Pseudonymisation. The GDPR introduces a new concept of "pseudonymisation" (that is, the processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual, without additional information). Pseudonymous data will still be treated as personal data, but possibly subject to **fewer restrictions on processing,** if the risk of harm is low.	Positive	EU-wide guidelines are expected to be produced, unifying the current disparate approaches. Businesses should keep this issue under review.
Binding Corporate Rules (BCRs). BCRs are agreements used to lawfully transfer personal data out of the European Economic Area (EEA).	Unclear	This is not expected to apply to insurer or IFA clients, but specific advice should be sought.
The right to erasure ("right to be forgotten"). Individuals will have the **right to request that businesses delete their personal data** in certain circumstances. It remains unclear precisely how this will work in practice.	Negative	Businesses will need to devote additional time and resources to ensuring that these issues are appropriately addressed.
The right to object to profiling. In certain circumstances, individuals will have the right to object to their personal data being processed (which includes profiling).		The impact of these restrictions on a given business will largely depend on how frequently that business engages in profiling activities.
The right to data portability. Data subjects have a new right to obtain a copy of **their personal data from the data controller in a commonly used and machine-readable format.**		All businesses should keep this issue under review. Businesses that process large volumes of personal data (for example, social media businesses, insurance companies, banks) should consider how they will give effect to these rights.
Data subject access requests. Business must reply within one month from the date of receipt of the request.		Businesses should plan how they will respond to data subject access requests within the new timescale and how they will provide the additional information required.

ROBERT WHARTON
Consultant Solicitor

M: 07836 678 134
T: 020 3319 3700
E: robert.wharton@keystonelaw.co.uk

CLICK HERE TO VIEW PROFILE