HRC Law TEAM

GDPR: Summary of Key Changes

A	**Accountability:** This new concept requires controllers to be able to demonstrate compliance with the Principles. This will shift the burden of proof onto the controller and is the basis for the new requirements on record keeping, keeping individuals informed and embedding data protection in your business.
R	**Requests from Data Subjects for Access (DSARs):** You will have to reply within one month and provide more information than was previously required. The first copy will have to be provided free of charge.
E	**Enforcement Powers increased**: Supervisory Authorities (**SAs**) will be able to impose fines on data controllers and data processors on a two-tier basis (depending on the type of violation) of: (i) up to 2% of annual worldwide turnover of the preceding financial year or 10 million euros (whichever is the greater); and (ii) up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever is the greater).
U	**Under an obligation to appoint a Data Protection Officer:** In certain circumstances, controllers or processors will be required to appoint a Data Protection Officer (**DPO**).
P	**Pseudonymisation:** This new concept involves processing personal data in such a manner that the personal data can no longer be attributed to a specific individual without additional information. The data will still be treated as personal data but may possibly be subject to fewer restrictions. This may also evidence accountability and privacy by design.
R	**Records:** You must maintain detailed documentation. Data processors must keep a record of processing activities. This does not apply to an organisation with less than 250 people unless processing is likely to result in a high risk to individuals.
E	**Expanded Territorial Scope:** If you process the personal data of **EU** citizens. For **non-EU** data controllers and data processors, you will be subject to the GDPR if you either: (i) offer goods or services to data subjects in the EU irrespective of whether payment is received; or (ii) monitor data subjects' behaviour insofar as their behaviour takes place within the EU.
P	**Privacy by design and by default.** Businesses will be required to implement data protection by design (e.g. when creating new products and services) and by default (e.g. data minimisation).

A	**Assessments re Privacy Impact (PIA):** Mandatory PIAs will be required before carrying out any processing that uses new technologies that are likely to result in a high risk to the data subject. Where PIA indicates a high risk to individuals, you must consult with the ICO before any processing takes place.
R	**Rights:** New or extended rights for data subjects include: Right **to be informed:** There will be an obligation to provide fair processing information where data is collected (and sometimes when received from a third party), typically through a privacy notice. The GDPR sets out the information that needs to be supplied. Right **to rectification**: Individuals will be entitled to have their personal data corrected if it is inaccurate or incomplete. Businesses must usually respond within one month of such a request. Right **to be forgotten**: Individuals will have the right to request that businesses delete their personal data in certain circumstances (i.e. where there is no compelling reason for the continued processing of that data). Right **to object to profiling**: In certain circumstances, individuals will have the right to object to their personal data being processed (which includes profiling i.e. online behavioural advertising and online tracing). Right **to data portability**: Individuals will have the right to obtain a copy of their personal data from the data controller in a commonly used and machine-readable format.
E	**Express consent**: New higher standards regarding consent will be required. Consent to process an individual's personal data must be given by a clear affirmative action for each processing purpose such as a written or oral statement (e.g. ticking a box on a website). It must also be unambiguous, freely given and with all required information provided.
D	**Data Breach Notification:** Businesses must notify the ICO of all data breaches within 72 hours unless the data breach is unlikely to result in a risk to the individuals (certain exceptions can apply).
?	**HRC Law** would be happy to assist you or your business with any **GDPR** issues. Graham Hansen, Associate at HRC Law, can be contacted on 0161 358 0552 or at grahamhansen@hrclaw.co.uk. You can find out more about Graham and HRC Law at **www.hrclaw.co.uk**.