The General Data Protection Regulation (GDPR)/ Law Enforcement Directive (LED): Key changes from the Data Protection Act 1998

OVERVIEW OF KEY CHANGES

The General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED) will both apply from 25 May 2018. The Regulation will directly replace many of the provisions of our own data protection legislation (the Data Protection Act 1998 (DPA) in the UK). Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), however there are new elements and enhancements so there is a need to implement some new procedures and do some existing procedures differently. The LED applies directly to those UK bodies processing personal data for law enforcement purposes, which will include the Home Office.

The Data Protection Principles, as set out in the DPA, remain but they have been condensed into six, as opposed to eight, principles. Article 5 of the Regulation states that personal data shall be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Under the GDPR the supervisory authority has a number of new powers (for the UK the supervisory authority for GDPR is the ICO). This includes an increase in the upper limit for fines from up to £500,000 or 1% of annual turnover to an upper limit of 20 million euro or 4% of global annual turnover, whichever is higher (for some infringements and an upper limit of 10 million euro or 2% of

global annual turnover for others). In addition an ability to issue warnings, carry out audits, require specific remediation (financial compensation), order erasure of data and suspend data transfers to a third county. Their powers extend to the right to enter premises for the purposes of monitoring compliance. Importantly some of these powers can be applied to data processors and controllers, see table below for further information.

So what does this means in practice? You will need to continue to manage and protect information as you do now, whilst also implementing some new procedures. You need to ensure you are aware of the changes that may affect your business areas outlined in the below table.

The DPA says	The GDPR/ LED says	Suggested Action Plan
Subject access requests must be responded to within 40 calendar days	Respond to SARs electronically and in a commonly used format within one month [the Cross Government view is that this equates to 30 calendar days and (in effect) 20 working days], extendable by a further two months (conditions apply), providing some additional information such as the data retention periods and the right to have inaccurate data corrected.	Update policy/guidance/ procedures. Plan how requests will be handled within new timescales identify how/what additional information must be provided. Continue to manage customer SARS through the Subject Access Request Unit, seeking to respond within new timescales and manage all staff requests through KIMU. Continue to provide data electronically.
Organisations are permitted to charge a reasonable fee for data requests.	Personal data requests will be free. Organisations can charge a reasonable fee or refuse a request if requests become manifestly unfounded or excessive. Fee must be proportionate to the cost of administration.	Update policy/ guidance/ procedures, to include different grounds for refusing to comply with a SAR (manifestly unfounded or excessive requests can be charged for or refused).

The DPA says	The GDPR/ LED says	Suggested Action Plan
Data subjects have a right to be informed: • what data is held on them • the purpose it is being processed for • who it may be shared with	Inform data subjects of the legal basis for processing their data. To include: • who the data controller is • how their data will be held • data retention periods • who data will be shared with • how to gain access to it • the right to complain to the ICO if they think data is handled incorrectly	Review and update all privacy and fair processing notices
Data breach reporting is only mandatory if the breach is covered by the Privacy and Electronic Communications Regulations 2011 and is noted as an advisory step for organisations outside of the PECR.	All data breaches where it is likely to result in a risk to the rights and freedoms of individuals must be notified by the data controller (Home Office) to the relevant supervisory authority (in most instances the ICO) within 72 hours. Any delay to this timeframe must be communicated to the ICO. If the data breach is likely to result in a high risk to an individuals' rights and freedoms the data subject must also be informed without undue delay (some exceptions apply).	Appoint a DPO with a supporting office to act as a point of contact for the reporting of breaches to the ICO [to be confirmed]. The DPO will be supported by a DPP network who will be the first point of escalation for business areas. Breach reporting instructions to be included within policy and guidance. Determine what constitutes high risk.
Under the current legislation there is no need for any business to have a dedicated DPO	A DPO is mandatory for any business or organisation with more than 250 employees The DPO should report to the highest management level of the controller or processor.	HO will recruit a DPO at SCS level with office support function

The DPA says	The GDPR/ LED says	Suggested Action Plan
There is no requirement for an organisation to remove all data they hold on an individual	An individual will have the 'Right to erasure' (with all information being permanently deleted) – which comprises all data including web records and portability (provide the personal data in a structured, commonly used and machine readable form).	Only applies to data obtained by data subject consent; if the majority of data collected by the organisation is not done by customer consent, ,these obligations will not apply to much of the data the organisation holds.
Privacy Impact Assessments (PIA) are not a legal requirement under DPA but has always been 'championed' by the ICO	Data Protection Impact Assessments (DPIA) will be mandatory and must be carried out when there's a high risk to the individuals freedoms, and in particular should be undertaken prior to commencing processing of personal data on new technologies DPIAs help an organisation to ensure they meet an individual's expectation of privacy.	The DST will be replaced with a DPIA and will be required for all instances of all data processing (not restricted to sharing) where the privacy of an individual or individuals is potentially impacted. Ensure DPIAs considered for all changes, new projects and integral to Change Management
Data collection does not necessarily require an opt-in under the current Data Protection Act	Consent is key. Individuals must actively opt-in whenever data is collected and there must be clear privacy notices. Notices must be concise, transparent, with consent able to be withdrawn at any time	To review all instances where customer consent is the legal basis for processing

The DPA says	The GDPR/ LED says	Suggested Action Plan
Liability for data breaches remains with the data controller where a controller uses a third party to act as a data processor (under legally binding contract).	The GDPR places new legal obligation on data processors including a requirement to maintain records of personal data and processing activities. Data processors have significantly more liability in the event of a data breach. Liability can fall to any party unless one can prove that it is not in any way responsible A controller may seek redress from a processor. As a data controller GDPR places further obligations on you to ensure your contracts and processes comply with the GDPR.	Identifying existing contracts, working with commercial to review and ensure compliance. Ensure MoU's are clear regarding the use of data and who is data controller/processor.
Under the DPA there is no special protection for children's personal data.	Special protection for children's personal data, particularly in the context of commercial internet services (e.g. social networking). If an organisation offers online services to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. At age 16 a child can give their own consent (although this may be lowered to a minimum of 13 in the UK).	Continue to operate our safeguarding procedures. Ensure privacy notices are written in language that children will understand.
Every data controller must lodge a formal notification document with the ICO outlining how personal data will be processed by that controller.	The current system of notification under the DPA will be replaced by a requirement for data controllers to keep their own record in relation to all the personal data they process; this must include; details of the purpose of processing; recipients; transfers to third countries; time limits for erasure and a general description of the technical and organisational measures in place to protect personal data.	Establish this document as a result of the data mapping exercise and identify a central resource within the organisation to manage and maintain it.

LED only changes

The DPA Says	The LED says	Suggested Action Plan
No logging requirement under the DPA. This relates to the ability of the data controller to maintain an audit of how personal data is being processed, including gathered, accessed, shared, stored and destroyed.	Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged so that this identification can be used to establish the justification for the processing operations. Logs should solely be used for verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.	Identify all the systems processing personal data, analysing existing logging capacity, identifying gaps and mitigating risks. Priority will be given to business critical systems.