General Data Protection Regulation - summary of main provisions

Introduction

The EU regulation known as General Data Protection Regulation ("GDPR") will come into force on 25 May 2018. The Government has also confirmed that it will introduce new legislation to repeal the Data Protection Act 1998 ("the 1998 Act") and to ensure that new UK legislation does not create inconsistencies with the GDPR. It therefore seems likely that new UK legislation would be introduced before or on 25 May 2018.

Purpose of GDPR

GDPR contains terminology that councils will already be familiar with because they are included in the 1998 Act (see Legal Topic Note 38) e.g. personal data, data controller, data processor, data subject, subject access request, processing, and data protection principles.

GDPR builds on the legal framework established by the 1998 Act to balance the needs of organisations (businesses, not for profit and public bodies e.g. local authorities) in their capacities as data controllers and data processors to collect and use personal data against the rights of an individual to have his information (personal data) kept secure and private. GDPR has been introduced to address the privacy issues arising from a digital age in which personal data may be collected, transmitted, stored, manipulated and shared with relative ease e.g. using emails, websites, the internet and the cloud.

The purpose of the GDPR is to increase (i) the obligations on organisations when acting as data controllers and (ii) the rights of individuals to ensure that their personal data is respected and used only for legitimate purposes. It also imposes new obligations on data processors.

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Put simply, personal data is data that relates to a living individual who can be recognised from that data. The categories of personal data processed by a council may include:

- communications with individual local residents including letters, complaints and council surveys;
- the council's employment and recruitment records (e.g. employment contracts, and job applications);
- contracts with individuals and contracts which require processing of personal data;
- arrangements with volunteers;
- communications with third parties e.g. principal authorities, CALCs, local charities, sports clubs, Disclosure and Barring Service ("DBS"), HMRC and staff pensions provider;
- the electoral roll and
- legal proceedings or transactions with individuals.

Summary of changes being introduced by GDPR

The annex to the Briefing provides a summary of the main provisions in the 1998 Act and the changes to be introduced by GDPR which are relevant to councils.

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

ANNEX

Subject	1998 Act requirements	GDPR requirements
Data protection principles	8 principles set out in Schedule 1.	Same principles in 1998 Act but condensed to 6 principles listed below. Personal data must be: • Processed fairly, lawfully and in a transparent manner in relation to the data subject. • Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. • Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. • Accurate and, where necessary, kept up to date. • 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. • Processed in a manner 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 (Article 5).

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Subject	1998 Act requirements	GDPR requirements
Consent	Data Controllers are required to have valid purpose(s) for processing personal data and where the data controller is relying on an individual's consent, this is referenced in para 1 of schedule 2 (in respect of personal data) and in para 1 of schedule 3 (in respect of sensitive personal data-consent must be explicit).	Data controllers are required to have legitimate reason(s) for processing personal data and where the data controller is relying on an individual's consent, the data controller must be able to demonstrate that consent, by a statement or by a clear affirmative action, was freely given, specific, informed and unambiguous for each purpose that it being processed. Prior to giving consent, the individual shall be informed of his right to withdraw his consent at any time. In other words, it should be as easy to withdraw consent as to give it (Articles 4 and 7).
Consent for children	The 1998 Act does not specify an age at which a child will be considered able to give consent, and it is left to a data controller to decide, on a case by case basis, whether a child has the ability to understand the concept of their personal data and whether the consent given by the child is informed consent (i.e. is understood).	Limits the ability of a child under 16 to consent to their personal data being processed in respect of "information society services" e.g. online businesses or social networking sites. This means where personal data is being processed for a child under 16, consent must be obtained from the child's parent or custodian. An EU member state may lower the age that a child can give consent to processing of their data from 16 to 13. (Article 8). On 7 August 2017, the Government announced that it would use the Data Protection Bill to legislate that children aged 13 years or older can consent to their personal data being processed for information society services (see Legal Briefing L04-17 for more information about the Bill).

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Subject	1998 Act requirements	GDPR requirements
Privacy notices (also known as fair processing notices)	Specifies basic information to be given by a data controller in a privacy notice (paras 1 – 5 of Part II of Schedule 1).	More information to be given by data controllers in privacy notices. This includes the following. • the identity and the contact details of the data controller and, if any, of the • controller's representative and of the data protection officer; • the purpose(s) of the processing; • the categories of personal data concerned; • the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations; • where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period; • the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; • the right to lodge a complaint with the ICO and • where the personal data is not collected from the data subject, any available information as to its source (Articles 13 and 14).

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Subject	1998 Act requirements	GDPR requirements
Communications by data controllers		There are new requirements on the data controller regarding the communications in a privacy notice and to the data subject relating to the rights of the data subject. Information provided must be a concise and intelligible form using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means (Article 12).

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Subject	1998 Act requirements	GDPR requirements
Data controllers working with Data processors	Where personal data is processed by a data processor on behalf of a data controller, the data controller must (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and (b) take reasonable steps to ensure compliance with those measures. Where processing of personal data is carried out by a data processor on behalf of a data controller, the processing shall be carried out under a written contract under which (a) the data processor is to act only on instructions from the data controller, and (b) the data processor must comply with obligations equivalent to those imposed on a data controller by the seventh principle. (Paras 11 and 12 of Part II of Schedule 1)	The data controller is required to enter into a contract with the data processor which imposes the following obligations on the processor: • Process the personal data only on the documented instructions of the controller. This is likely to mean that data processors cannot use cloud computing technology or services without the data controller's approval. • Comply with security obligations equivalent to those imposed on the controller under Article 32 of the GDPR. • Only employ staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality. • Enlist a sub-processor only with the prior permission of the controller. • Assist the controller in carrying out its obligations with regard to requests by data subjects to exercise their rights under Chapter III of the GDPR (including the right to transparency and information, the data subject access right, the right to rectification and erasure, the right to the restriction of processing, the right to data portability and the right to object to processing). • Assist the data controller in carrying out its data security obligations under Articles 32 to 36 of the GDPR (Article 28).

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Subject	1998 Act requirements	GDPR requirements
Privacy Impacts assessment (PIA)	A PIA is a process which helps an organisation to identify and reduce the privacy risks of new projects (e.g. use of CCTV or an IT system/ database for storing and accessing personal data) or policies. Conducting a PIA is not a requirement of the 1998 Act but it is regarded as good practice by the ICO. The ICO has issued a code of practice in respect of PIAs (s .51).	Where a type of processing in particular uses new technologies and the purpose(s) that the data controller wishes to process personal data poses high risks, it will have to carry out a data protection privacy impact assessment before such processing (Article 35). The ICO is expected to provide guidance about the type of processing that would demand a data protection privacy impact assessment.
Notification by data controllers	Notification to ICO to be included in register of data controllers (s.18).	The requirement to provide notification to ICO is replaced by a new requirement for data controllers to maintain a written record of processing activities under their responsibility. The written record shall include a description of the categories of data subjects and the categories of personal data, purpose(s) of processing, categories of recipients of personal data, time limits for erasure and description of technical and organisational measures to protect data. Data processors also have a new duty to maintain a written record of similar information. However, the obligation to maintain a written record does not apply to an organisation employing less than 250 persons unless the processing it carries out is likely to result in risks to the rights of data subjects, the processing is not occasional, or the processing includes special categories of data e.g. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, or processing criminal convictions and offences. (Article 30).

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Subject	1998 Act requirements	GDPR requirements
Appointment of Data Protection Officer (DPO)	No requirement.	Data controllers and data processors must designate a DPO in 3 situations which include where the processing is carried out by a public authority or body (e.g. local authorities including a parish council or, in Wales, a community council) (Article 37).More information about the DPO is in Legal Briefing L04-17.
Notification to report personal data breaches	No requirement.	Data controllers are required to report to the ICO personal data breaches without delay and within 72 hours. A data processor must also notify a data controller without undue delay after becoming aware of a personal data breach (Article 33).
Fines	ICO may fine a data controller up to £500,000 for serious breaches (s.55A).	There are heavy fines for data controllers and data processors for a wide range of breaches. Some breaches (e.g. failing to comply with data subjects' rights or the principles for processing including conditions for consent) attract fines of up to 4% of annual turnover for the preceding year or 20 million Euros whichever is higher. For other breaches (e.g. failing to keep records of processing activities, to appoint a DPO or to comply with security obligations) the fine can be up to 2% of annual turnover or 10 million Euros, whichever is higher (Article 83).

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Subject	1998 Act requirements	GDPR requirements
Individuals' rights	Individuals have certain rights against data controllers	Existing rights are strengthened and new rights are given. Individuals also have (limited) new rights against data processors.
	• The right of access to personal data held by a data controller within 40 days of request upon payment of £10 fee (s.7).	The right of access to personal data held by a data controller must be dealt with within one month of request and free of charge. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the data controller may charge a fee for providing the information or refuse to respond (Articles 12 & 15).
	• The right to prevent processing likely to cause damage or distress (s.10).	The right to restriction of processing (Article 18).
	• The right to prevent processing for purpose of direct marketing (s.11).	The right to object to the processing of personal data for direct marketing purposes (including profiling to the extent that it is related to direct marketing) (Article 21).
	• The right to object to decisions being taken by automated means (i.e. by a computer, by online profiling) (s.12).	The right not to be subject to automated decision-making (Article 22).
	• The right to claim compensation for damages caused by a breach of the 1998 Act (s.13).	The right to receive compensation from the data controller is retained and there is a new right to receive compensation from the data processor for the damage suffered as a result of an infringement of GDPR (Article 82).

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Subject	1998 Act requirements	GDPR requirements
Individuals' rights	• The right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed (s.14).	The right to obtain from a data controller without undue delay the rectification of inaccurate personal data (Article 16). There is a new right to erase personal data (also known as the "right to be forgotten") which means that data subjects will be able to request that their personal data be erased by the data controller and no longer processed. This will be where the data is no longer necessary in relation to the purposes for which it is processed, where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with GDPR. However, the further retention of such data will be lawful in some cases e.g. amongst others, where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims. Where the data controller has made the personal data public and is obliged to erase the personal data it shall take reasonable steps to inform data controllers which are processing the personal data that the data subject has requested them to erase any links to, or copy or replication of that personal data (Article 17).
	• None	A new right to be notified by a data controller when a personal data breach is likely to result in a high risk to a data subject's rights (Article 34).
	• None	A new right to data portability - to receive a copy of personal data or to transfer personal data to another data controller (Article 20).

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk

Further reading

The ICO's website has detailed guidance about:

- the new obligations for data controllers and data processors which can be accessed via https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/

  and

- the new rights for individuals which can be accessed via https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/

National Association of Local Councils
Tel: 020 7637 1865 • Fax: 020 7436 7451 • e-mail: nalc@nalc.gov.uk • website: www.nalc.gov.uk