Reform of data protection legislation- General Data Protection Regulation and Data Protection Bill

General Data Protection Regulation

As explained in Legal Briefing L03-17, the EU regulation known as General Data Protection Regulation ("GDPR") will come into force on 25 May 2018. As an EU regulation, the GDPR has direct effect; no national legislation is required for its provisions to apply. L03-17 confirmed that preparations for compliance with the requirements of GDPR will have significant resource implications for councils but should not be delayed. Compliance will be difficult if councils leave preparations until next year.

Getting ready for GDPR

1. With reference to L03-17 and the Information Commissioner Office's ("ICO") guide entitled "Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now" (available via the web link https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf), the 12 steps required by councils include the following.

   i) Ensuring that all councillors are aware that the law is changing and appreciate the impact this is likely to have. Councils should identify the activities/areas that could cause compliance problems under the GDPR.

   ii) Auditing and documenting the personal data that they hold, where the personal data came from and how it is used or shared. This exercise will require resourcing.

   iii) Identifying the lawful basis for processing and retaining personal data, documenting this and updating privacy notices. Under the Data Protection Act 1998 ("the 1998 Act"), a privacy notice is a reference to particular information which an organisation is required to provide to individuals when it is processing their personal data. This information includes confirmation of the identity of the organisation (i.e. the data controller) and, if any, the identity of the person processing personal data on behalf of the organisation (i.e. the data processor), the purpose(s) for which personal data will be processed and any other information which is necessary in the specific circumstances to enable the data processing to be fair. GDPR includes a longer and more detailed list of information that

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

must be provided in a privacy notice. GDPR also requires privacy notices to be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

Detailed advice about privacy notices is available from the ICO via https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/. It includes guidance about how to write privacy notices. The ICO has also compiled examples of good and bad privacy notices which can be accessed via https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf

iv) Reviewing how consents are sought, recorded, and managed. There is a fundamental difference between telling individuals how their personal data will be used and obtaining their consent for the same. Consents to a council must be freely given, specific, informed and unambiguous. There must be a positive opt-in consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and there must be simple ways for people to withdraw consent.

v) Recruiting/procuring the services of a Data Protection Officer ("DPO") who is required by GDPR to have expert knowledge of data protection law and practices. To clarify L03-17, GDPR requires "public authorities" (which includes local authorities such as parish councils and, in Wales, community councils) to appoint a DPO. More information about the DPO is in the Annex.

2. Councils may use the ICO's self-assessment exercise in respect of compliance with GDPR. This is available via https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/.

3. Councils should use the ICO's website for detailed and practical guidance about GDPR via https://ico.org.uk/for-organisations/data-protection-reform.

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

Data Protection Bill

At the opening of Parliament on 21 June 2017, the Government committed itself to the introduction of the Data Protection Bill. Parts of the 1998 Act would need to be repealed for data processing to be within the scope of the GDPR and it is necessary to ensure that the 1998 Act does not duplicate or create inconsistencies with the GDPR, because the GDPR will be directly applicable.

In respect of the Data Protection Bill, the Government said its key priorities were:

- ensuring data protection rules were "suitable for the digital age";
- empowering individuals to have more control over their personal data;
- giving people the "right to be forgotten" when they no longer wanted an organisation to process their data - providing there were no legitimate grounds for an organisation retaining the data;
- modernising data processing procedures for law enforcement agencies;
- allowing police and the authorities to "continue to exchange information quickly and easily with international partners" to fight terrorism and other serious crimes;
- ensuring the country met its obligations while a member of the EU, and would help the UK maintain its "ability to share data with other EU members states and internationally after we leave the EU" and
- replacing the 1998 Act.

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

a) What are the DPO's responsibilities?

The DPO's minimum tasks are defined in Article 39 of GDPR. These are below.

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits and
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

The DPO will therefore have an "internal' and "external' aspect to their role, and it will be important that these do not interfere with one another.

The appointed DPO must at all times have regard to "the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing." This is an overarching obligation which means that the role of the DPO will vary in proportion to the risks to the rights of individuals affected by the organisation's processing of personal data.

A DPO is not personally responsible in case of non-compliance with GDPR. Article 24 of GDPR makes it clear that data protection compliance is a responsibility of the data controller or the data processor.

b) Who may be appointed as the DPO?

Article 37(6) of the GDPR provides that the DPO may be an employee or external to the organisation, fulfilling the tasks on the basis of a service contract.

Where an employee is chosen as the DPO, there is nothing to prevent that individual from also performing other roles at the organisation, provided such roles do not affect his ability to adequately perform the role of DPO. The appointment of an internal DPO may also raise confidentiality and conflict of interest issues, and it will be important for organisations to develop policies and procedures to manage any such issues.

If the DPO is external, his function can be exercised based on a service contract with an individual or an organisation. Where an external DPO is selected, it will be

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

important for organisations to ensure that the DPO is able to form productive relationships with internal stakeholders and colleagues in order to perform the DPO role adequately.

c) Does the DPO need specific qualifications?

Article 37(5) of the GDPR provides that the DPO shall have expert knowledge of data protection law and practices. This should be proportionate to the type of processing that the organisation carries out, taking into consideration the level of protection the personal data requires. In the case of a public authority, the DPO should have sound knowledge of the organisation's administrative rules and procedures.

The DPO's relevant skills and expertise should ideally include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR;
- understanding of the processing operations carried out;
- understanding of information technologies and data security;
- knowledge of the business sector and the organisation and
- ability to promote a data protection culture within the organisation.

d) Resources for DPO

Article 38(2) of the GDPR provides that depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- active support of the DPO's function by senior management ;
- sufficient time for DPOs to fulfil their tasks;
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate;
- official communication of the designation of the DPO to all staff;
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services and
- continuous training.

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