CAMBOURNE PARISH COUNCIL

District of South Cambridgeshire

Council Meeting 5th September 2017

Reform of Data Protection Legislation – General Data Protection Regulation And Data Protection Bill

The European Union has issued new a regulation known as the General Data Protection Regulation which will come in to force on 25th May 2018. This potentially has some onerous implications for Parish Councils and it was felt appropriate to give early notice of the new regulation. Attached is the NALC Legal Briefing L04-17 which gives an outline of what is expected. The Cambridge branch of the SLCC is organising Clerk's training at the December branch meeting due to the importance. However, CaPALC will not be in a position to provide training until March next year. It may be appropriate to rearrange the October or November Councillor Training session to cover the new regulation.

Documents attached:

- NALC Legal Briefing L04-17
- The Information Commissioner's Office (ICO) publication Preparing for the GDPR, 12 steps to take now.

It is:
RECOMMENDED that the Parish Clerk arrange appropriate training for all councillors.

AGENDA ITEM No. 13

NALC

Legal Briefing
L04-17
July 2017

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.

© NALC 2017

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.

© NALC 2017

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

AGENDA ITEM No. 13

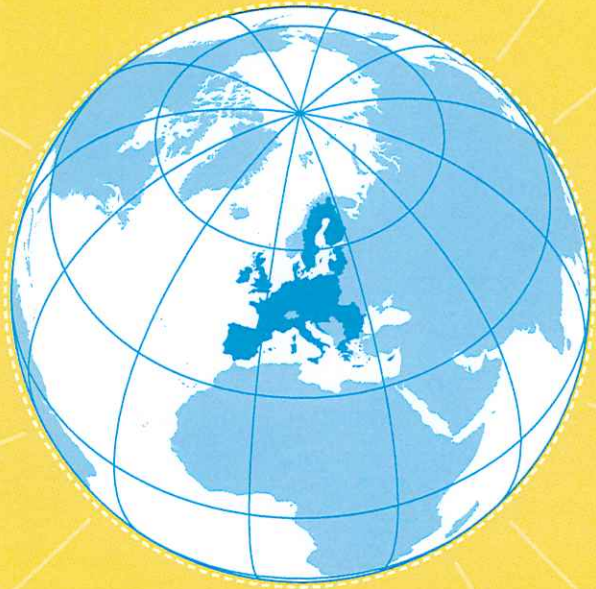
Preparing for the General Data Protection Regulation (GDPR)

12 steps to take now

ico.

Information Commissioner's Office

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now



1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico.
Information Commissioner's Office

ico.org.uk

V2.0 201705

Introduction

This checklist highlights 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

It is important to use this checklist and other Information Commissioner's Office (ICO) resources to work out the main differences between the current law and the GDPR. The ICO is producing new guidance and other tools to assist you, as well as contributing to guidance that the Article 29 Working Party is producing at the European level. These are all available via the ICO's Overview of the General Data Protection Regulation. The ICO is also working closely with trade associations and bodies representing the various sectors – you should also work closely with these bodies to share knowledge about implementation in your sector.

It is essential to plan your approach to GDPR compliance now and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this document will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

Some parts of the GDPR will have more of an impact on some organisations than on others (for example, the provisions relating to profiling or children's data), so it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process.

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to

complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

The ICO's Privacy notices code of practice reflects the new requirements of the GDPR.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form and provide the

information free of charge.

5 Subject access requests

You should update your procedures and plan how you will handle requests to take account of the new rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to

help you comply with the GDPR's 'accountability' requirements.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

You should read the detailed guidance the ICO has published on consent under the GDPR, and use our consent checklist to review your practices. Consent 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 you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society 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. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

10 Data Protection by Design and Data Protection Impact Assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

You should also familiarise yourself now with the guidance the ICO has produced on PIAs as well as guidance from the Article 29 Working Party, and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- a public authority (except for courts acting in their judicial capacity);
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions. The Article 29 Working Party has produced guidance for organisations on the designation, position and tasks of DPOs.

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

12 International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – ie you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states.

If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

The Article 29 Working party has produced guidance on identifying a controller or processor's lead supervisory authority.