Impact of new General Data Protection Regulations (GDPR)

PURPOSE OF REPORT

1. To inform the Council of the implications of the General Data Protection Regulation (GDPR) that is planned to take effect from May 2018! The parish Council needs to consider how best to meet its legal obligations with special regard to the security of data held by the Council, and communications by and between Parish Councillors, Officers and the public**.**

RECOMMENDATION

2. **It is RECOMMENDED that:-**

   a. the Council reviews the twelve steps outlined by the Information Commissioner's Officer (Appendix A) and assesses relevance and actions to be taken by May 2018, and reports back to the next meeting in February,

   The Council needs to improve its Awareness of what the GDPR means in practical terms and how can it demonstrate it has acted 'reasonably' (if that is considered to be a 'defence'?) HALC have arranged a series of four training seminars between November and March (see Appendix B).

   b. the Clerk/DPO AND Cllr Jan Hertz attend one of the HALC training courses. The rationale for the latter attendee is that many of the key components of compliance with GDPR relate directly to the appropriateness of HPC's IT data storage/access and IT communications security.

BACKGROUND

3. GDPR is designed to enable individuals to better control their personal data.

4. The GDPR was ratified mid 2016 and immediately became law. European Union Member states have a 2 year implementation period. Enforcement will commence by 25th May 2018 at the latest. The Government has given a commitment that post Brexit the requirements of the EU legislation will be embodied in UK Law.

5. The 'document' summarises the key components of the GDPR – it should be noted that this is only a simplified summary and that the full text (all 204 pages) contains much more detail! Despite this morass of information, at the Basingstoke and Deane Association of Parish and Town Councils (BDAPTC) meeting 21st November, it was clear there were a large number of, as yet, unknowns. There is still uncertainty with regards the expectations, requirements, funding implications, funding support, detailed application, scrutiny and enforcement!

6. These are some of the key points identified by NALC's Chief Executive in his Bulletin 41 - 17 November 2017. "This week I wrote to the Department for Digital, Culture, Media and Sport to set out our latest concerns about the impact of the General Data Protection Regulation on our councils. In my letter strongly worded letter I called for:-
   - an urgent update on progress developing sector specific guidance and

- our request for financial assistance to meet the cost burden **in particular appointing a Data Protection Officer**,
- registered my deep concern about the lack of contact from DCMS and the Information Commissioners Office,
- requested the new helpline for small businesses be made available to our councils, and,
- raised again whether clerks can be the DPO.

7. Attendees at the BDAPTC, were advised that the best website from which to get background information is the one provided by the ICO Guide… *"explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection. This is a living document and we are working to expand it in key areas."*

8. The final statement above reinforces that the current GDPR, due to be implemented by May 2018, is not yet finalised. Nevertheless, the ICO Guide does include TWELVE STEPS (See Appendix A).

Does GDPR, whatever it is, apply to Hannington Parish Council?

9. **The simple answer is YES**, as exemplified in the statement regarding appointment of a Data Protection Officer?

10. An early draft of the GDPR limited mandatory data protection officer appointment to organisations with more than 250 employees, the final version has no such restriction. This is where the NALC question, "can Clerks be the DPO?" Currently the Clerk is designated the DPO and FOI (Freedom of Information Officer). If not, then HPC is placed in an absurd decision; unless a 'central DPO' was appointed by NALC/HALC/BDBC and recovered a proportion of the costs from the Parish Council

11. The absurdity of not applying a 'de minimus' is that *'Regulators will now have the authority to issue penalties equal to **THE GREATER OF** 10 million Euros or 2% of the entity's global gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessments.*

Data Storage and Communications Security

12. Discussions at the BDAPTC centred around:-

Data storage: how secure are Parish council's data storage and websites? Suggestion was that parish councils should make use of access to central government's 'G cloud' with its high level security.

Communications: once again suggestion was to use the more secure web addresses of '…@ … gov.uk' and not '…co.uk'. The Clerk and ALL Councillors should be allocated these web addresses and ALL communication on behalf of the PC MUST be made through these addresses. Lower secure networks could enable a hacker, once in the email address would then have access to the parish council's database and website; from which unlawful emails could then be sent to public and businesses. Only the Cllr and the Clerk would have access to the Councillors emails. If the Cllr 'lost' an email etc , he/she would have to ask the Clerk to undertake a search.

Once a councillor left the parish council, they would NO LONGER have access to the … @...gov.uk email address and would therefore also lose ALL access to their previous Council emails etc.

IT hardware: a further step by one of the large proactive parish councils in ensuring 'security' and compliance with GDPR was to issue each Cllr with a 'notepad?', which had to be handed in at the end of their period as Clerk. This 'notepad' was NOT for personal use.

Chris Pottinger,
Clerk, Hannington Parish Council
22nd November 2017

APPENDIX A

Information Commissioner's Office- Twelve Steps

STEP 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.

STEP 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.

STEP 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.

STEP 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.

STEP 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.

STEP 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.

STEP 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, preticked 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.

STEP 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.

STEP 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.

STEP 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.

STEP 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.

STEP 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.

APPENDIX B

HALC Training: General Data Protection Regulation

Recommended for: Councillors, Officers responsible for Data Protection and Data Protection Officers.

Session overview:

This essential session will clarify what the new data protection regulations are, what they mean for you and your council, and the action that you need to take. With both taught and interactive elements, there's also the opportunity to gain insight and understand the implications of the new regime in broader terms and contrast to what you already do.

Session benefits:

By the end of the session you will:

- Learn About Changes to Data Protection coming in shortly
- Gain understanding of the additional impact for your Council
- Equip yourself with the skills to ensure your Council is fully compliant
- Have the opportunity to gain ideas from other Town and Parish Councils

Session leader: Dawn Hamblet

Price per delegate: £ 40 + VAT for Hampshire ALC members. For non-member price please see LCPD Training & Events Terms & Conditions. This price includes hot drinks and session notes.

To book now please complete a booking form or for more information contact Sue Ramage.

Please Note: Submission of a booking request will amount to your acceptance of the LCPD Training & Events Terms & Conditions.

In-house training

This session can be provided in-house, which is a cost-effective approach if you have a number of people who require training. You choose where and when you want our trainers to deliver. We will also tailor the course content to suit your precise organisation needs.

To find out more about LCPD in-house training, please see our In-House Training web page or to speak us about your particular requirements please contact Sue Ramage.