COTHERSTONE PARISH COUNCIL

General Data Protection Regulations

Author Clerk / Responsible Finance Officer
Meeting date 14 February 2018

Introduction

The law is changing. The regulation known as General Data Protection Regulation (GDPR) will come into force on 25 May 2018. The UK Government will introduce new legislation to repeal the Data Protection Act 1998 and to ensure that new UK legislation does not create inconsistencies with the GDPR.

The purpose of this paper is to provide background information to councillors and to enable a discussion on the Parish Council's preparations for the introduction of GDPR.

Purpose of GDPR

GDPR builds on the legal framework established by the 1998 Data Protection Act to balance the needs of organisations (businesses, not-for-profits and public bodies), in their capacities as data controllers and data processors to collect and use personal data, against the rights of an individual to have their 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 eg. using emails, websites, the internet and the cloud. The purpose 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.

Implications for the Parish Council

The major impact for the Parish Council will be the need to have documentation to demonstrate its accountability in respect of data protection. Many things the Council is doing already comply with the current Data Protection Act.

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.

Lots of the concerns and implications for larger organisations are connected with the automatic processing of data. Although the Parish Council holds personal data on computer systems, there is very little automatic processing involved.

Practical steps the Parish Council will need to take

1. When the Parish Council requests or receives any personal data it should issue a privacy notice setting out: the Parish Council identity, how it intends to use the information, the lawful basis for processing the data, the Council's data retention period and the fact that individuals have a right to complain to the Information Commissioner's Office if they think there is a problem with the way the council is handling their data. This privacy notice must be provided in concise, easy to understand and clear language.

   The Parish Council must have a Subject Access Request procedure setting out how it will handle any request from an individual about the data it holds on them.

2. The Parish Council should prepare a document which describes the personal data it processes.

   Personal data held by the Parish Council falls into the following eleven categories. Where information other than contact details is held, this is mentioned specifically.

   - Electoral Register (including unique electoral identifier)
   - Cemetery records
   - Allotment records
   - Common Land Registration records
   - Councillors' details (including Register of interests)
   - Suppliers to the Parish Council (if individual, not corporate, including bank account details)
   - External organisation contacts / Community organisations
   - Contractors (where individuals can be identified rather than a corporate body)
   - Employee (Clerk) (including National Insurance Number)
   - Business contacts (eg. CDALC, SLCC)
   - Local residents / electors

   For each category of data, the following will be recorded:

   a. What data is held
   b. Where the data came from
   c. How the data was obtained / consent sought
   d. Why the data is needed
   e. The lawful basis for processing this data
   f. With whom the data is shared by the Parish Council
   g. What would constitute a data breach requiring notification to the ICO or affected individuals

   A skeleton of such a document is provided at Appendix 1.

3. The Parish Council should prepare a consent mechanism for each of the above categories of data, using a checklist offered by the Information Commissioner's Office. Consent to hold an individual's data 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, and there must be a simple way for people to withdraw their consent.
4. As the Parish Council does not process any data for individuals under 16, specific systems to verify individuals' ages, other than 'over 16' will not be necessary.
5. The Parish Council needs a procedure in place to detect, report and investigate any personal data breach (failure to report a breach could result in a fine, as well as a fine for the breach itself).

Note that if 'consent' is given as the lawful basis for processing personal data then those individuals have a right to have their data deleted.

Data Protection Impact Assessment / Privacy Impact Assessment

Data Protection Impact Assessments are mandatory in certain circumstances 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 individual, or where there is processing on a large scale. Data processing by the Parish Council is not considered to meet these criteria and therefore a Data Protection Impact Assessment is not necessary.

Appointment of (external) Data Protection Officer

As a public authority, the Parish Council is required to formally designate a Data Protection Officer (DPO). The DPO must take responsibility for the Parish Council's data protection compliance and have the knowledge, support and authority to carry out their role effectively.

The minimum tasks of an organisation's DPO will be:

- 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 impact assessments, train staff and conduct internal audits;
- To be the first point of contact for the Information Commissioner's Office and for individuals whose data is processed.

Whilst the DPO *can* be appointed from within an organisation or as an external data protection adviser, clear advice from the National Association of Local Councils is that a Parish Council's Clerk/RFO should NOT be designated as DPO, nor a councillor unless they have expert knowledge of data protection law and practices.

Specifically, an 'internal' appointment (either Clerk or councillor) will not satisfy all of the requirements of the job because:

- There are conflicts of interests (which may arise from responsibilities as a clerk/RFO and may including processing activities);
- The need for independence;
- The need for expert knowledge of data protection law and practices; and
- The need for adequate time to perform DPO role.

Options which NALC are working on include to enable every council to have a DPO are:

a) County Associations (in our case CDALC) make available a list of reputable firms that understand the sector ('trusted suppliers') which council can then approach;

b) NALC work with a supplier to provide a national service which local councils then buy into as their appointed DPO (estimated annual charge £300-£350);

c) Setting up a sector-led body to provide a DPO service and other support, or a county-based structure with national co-ordination/support.

NALC has advised that option b) is the most immediately available and it has negotiated with a legal firm active in the public sector, who would set up an 'on-demand' DPO service which, at base, would cost £350 per annum for email support 5 days per week, with reply within 24 hours; and a schedule of fees for greater engagement.

It should be noted that, notwithstanding the remit of the DPO' responsibilities, regulations confirm that the Parish Council is responsible for compliance with data protection law, not the DPO.

Compliance

Given that there has been two years to prepare for the introduction of GDPR, there will be no 'grace period' — the Information Commissioner's Office (ICO) will be regulating from 25 May 2018. The ICO has also stated that it is a fair and proportionate regulator; those who self-report, engage with the ICO to resolve issues and who can demonstrate effective accountability arrangements can expect this to be taken into account when it considers regulatory action.

There are heavy fines for data controllers and data processors for a wide range of breaches. Some breaches (eg. failing to comply with an individual's rights, or the principles for processing, including conditions for consent) attract fines of up to 4% of annual turnover. For other breaches (eg. failing to keep records of processing activities or to appoint a DPO) the fine can be up to 2% of annual turnover.

It is the Parish Council's responsibility to ensure that it is compliant before 23 May.

Other sources of support

The National Association of Local Councils (and through the County Durham Association of Local Councils) has commissioned a GDPR Guidance Note or Toolkit for members, offering practical Action Plans, checklists and other useful documents as well as providing a plain English briefing on the new law ('available January 2018', but not yet received). The intention is that this toolkit will include consent forms, data rights checklist and template response letter, security incident response policy checklist, data processing checklist, GDPR checklist template, Data Protection Impact Assessment template and privacy notice templates.
NALC is also lobbying the ICO for sector-specific advice and support and for 'new burdens' funding to ease transition.

Recommendations

1. The requirements of the forthcoming introduction of General Data Protection Regulations are noted.
2. Council agrees to continue to monitor developments as necessary through the National Association of Local Councils and County Durham Association of Local Councils.
3. Councillors discuss and revise the draft GDPR framework document prepared by the Clerk (Appendix 1).
4. An external Data Protection Officer is appointed as soon as possible, and £350 is allocated in the 2018/19 budget for this purpose.

Sources

1. Preparing for the General Data Protection Regulation GDPR), Information Commissioner's Office, May 2017.
2. Society of Local Council Clerks, newsletter November 2017.
3. Information Commissioner Blog post, December 2017.
4. Email from Steve Ragg, CDALC, 20 December 2017.
5. NALC Legal Briefing L04-17, Reform of data protection legislation – General Data Protection Regulation and Data Protection Bill, July 2017
6. NACL Legal Briefing L05-17, General Data Protection Regulation – summary of main provisions, August 2017.
7. NALC's GDPR Activity Update, December 2017.
8. NALC L10-17, Data Protection Officer, 21 December 2017
9. NALC General Data Protection Regulation Appendix 8.1: National Assembly, 6 February 2018.

Cotherstone Parish Council

APPENDIX 1

General Data Protection Regulation

Personal data held by Cotherstone Parish Council

Category of data	What data is held	Where the data came from	How the data was obtained / consent sought	Why this data is needed	Lawful basis for processing this data (eg. consent)	With whom the data is shared	What would constitute a data breach?
Electoral Register for the parish	• Name / Address • Unique electoral identifier	Durham County Council	Emailed spreadsheet (password protected)	Eligibility for election or co-option to the Parish Council			
Cemetery records	• Name / Address / Email address	Individuals	From funerals directors / residents	Management of cemetery / grave plots			
Allotment records	• Name / Address / Email address	Individual tenants	Application from individuals	For allotment agreement	Consent		
Common Land Registrations	• Name / Address	Durham County Coucil	Correspondence				
Councillors details	• Name / Address / Email address / telephone numbers / Register of interests	Councillors	Paper proforma on election/co-option	• Internal correspondence • Public register of interests • Access to councillors by the public			
Supplier (if individual, not corporate)	• Name / Address / Email address / telephone numbers/ Bank account details	Business correspondence	Business correspondence	Business transactions			
External organisations	• Name / Address / Email address / telephone numbers	Eg. Play @ Cotherstone, Cotherstone Village Hall	??				

Contractors (where individuals can be identified rather than a corporate)	• Name / Address / Email address / telephone numbers/ Bank account details	Business correspondence	Business correspondence	Business transactions			
Employees	• Name / Address / Email address / telephone numbers/ National Insurance Number	Application form and payroll administration	Transferred from application form to PC systems				
Business contacts (CDALC, SLCC)	• Name / Address / Email address / telephone numbers	Contact with the individual	Business correspondence (most likely email)	To conduct PC business (eg. funeral directors)			
Local residents / electors	• Name / Address / Email address / telephone numbers	Letters, emails, webforms, telephone calls or completed surveys.	Incoming correspondence	Engagement with the PC			

Privacy Notice – draft contents

The following notice is given when personal data is collected by the Parish Council:

Identity: Cotherstone Parish Council

Data controller: The Clerk

Data Protection Officer for Cotherstone Parish Council: To be appointed

Legal basis for using the information:

Data retention period:

Right to complain: If you think there is a problem with the way we are handling your data, then you have a right to complain to the Information Commission. The contact details are: xxxx etc

What will happen if a data breach is identified:

Is a Data Protection Impact Assessment necessary: (if no, why not)

International considerations: The Parish Council does not operate in more than one EU member state.

Children: The Parish Council does not hold or process any data relating to children under the age of 16.