CODDENHAM PARISH COUNCIL

Annual General Meeting – 24th May 2018

Report to Council

Item 16. General Data Protection Regulations Policy

This report **Recommends** that Council delegate the drafting of a policy regarding the Council's responsibilities under the new General Data Protect Regulations to the Policy Review Working Group for consideration at an early future meeting of the Parish Council.

Introduction

Council is required to have policy and procedures in place to ensure compliance with the General Data Protection Regulations which come into force on 25th May 2018 and that these are reviewed annually.

The following information is taken from a training session provided at the SALC offices earlier this year, detailing the matters relevant to a policy and the work required in the development of the Council's governance documents in this regard.

The General Data Protection Regulation

What is GDPR? The General Data Protection Regulation comes into force on May 25th, 2018 and constitutes the biggest change in privacy legislation for over 20 years, repealing the Data Protection Directive 95/46/EC and overriding the Data Protection Act 1998.

Why has it been introduced?

- Needed to bring data protection laws into the social media age
- Effectively reverses ownership of personal data
- Gives control back to the individual
- Puts significant pressure on organisations to protect personal data from loss
- Encourages only the necessary data to only be stored and only for the duration necessary
- Obliges everyone to comply
- Restricts the movement of personal data outside of the EEA
- Imparts obligations on non-EEA organisations handling data on EU residents

Personal Data is any information relating to a person that can be used to directly or indirectly identify that person, such as: full name; email address; date of birth; IP address / website cookies; purchases; downloads; subscriptions and services used; questions and responses; promotions used; survey responses; financial history; banking/credit; payment transactions and donations; healthcare and education services used; CCTV recordings; gender identity; location data; credit card data; judgements/sanctions; government services capable of identifying an individual either on its own or when combined with other information; internal account numbers; PINs and passwords; IMEIs; National Insurance number; driving licence number; passport number.

Special category high risk data – Prohibited without explicit consent or reasons:

Race/ethnic origin; political opinions; religious beliefs and union membership; Biometric; genetic; health/medical data; Sexual orientation; sex life; Criminal offenses; criminal convictions.

A **Data Controller** is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

A **Data Processor** is the natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller: E.g. Your marketing agency; Research company; Payment service provider; Solicitors and accountants who you provide data to; Cloud / offsite backup / IT providers; HR or payroll agency; CCTV monitoring / site security companies.

Data subject is an identified or identifiable person.

Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Protection Officer (DPO) is a person within the organisation responsible for overseeing, policing and driving privacy. A DPO is required by all public organisations, those processing High Risk data or data on a 'large scale'

What Data falls under the GDPR? The GDPR affect both manual and automated processing, i.e. Databases; voice mail and completed forms; CCTV; cookies and website tracking. Includes both digital and paper records, so consider off-site secure storage. Only applies to personal data able to identify a living subject, so excludes anonymous and encrypted information. Applies to all 'data subjects' so affects public sector, Non-Governmental Organisations, Not for Profit, Business to Consumer and Business to Business transactions, customers, employees, Suppliers, Contractors etc

Principles. Data must be processed lawfully, fairly and transparently and only collected for explicit and lawful purposes. Data must be relevant and necessary for the purpose kept up-to-date and accurate or rectified. Keep data only if required and for no longer than necessary. Keep data secure.

Accountability -Article 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

1st Principle - Lawful Basis for Processing:

a) the data subject has given consent to processing
b) the performance of a contract…or to take steps… prior to entering into a contract
c) for compliance with a legal obligation to which the controller is subject
d) in order to protect the vital interests of the data subject
e) performance of a task carried out in the public interest or…official authority vested in the controller
f) for the purposes of the legitimate interests…, except where such interests are overridden by the interests…of the data subject…in particular where the data subject is a child

Individuals' rights

- 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 to processing,
  only if it causes unwarranted and substantial damage or distress
- The right to compensation if they suffer loss or damage

Penalties

Two-tiered sanctions from the ICO. Most serious violations €20 million or 4% of global turnover (whichever is greater). Lesser incidents max €10m or 2% global turnover (whichever is greater). Compares to max €600,000 for Data Protection Act 1998. ICO can carry out audits at any time. Demonstrating accountability will be key. No exemption for Force Majeure.

Costs relating to a breach

Fines are cumulative based on:

- Lack of documentation and evidence of compliance
- Inability to demonstrate an appropriate lawful basis for processing
- Inadequate security, safeguards or processes
- Failing to notify the ICO and (where necessary) Data Subjects of a breach
- Cost of brand and reputational damage
- Cost of investigating and rectifying the breach

Data subjects can sue for compensation via class action for "loss and distress". If a Data Processor is at fault, they are now equally liable along with Data Controllers. Insurance cover must be adequate.

Breach notification

You will need a breach reporting process:
You have 72 hours to report the breach to the regulator(s) (i.e. The ICO) from the point your become aware of it. Data subject notification only necessary where rights and freedoms affected. You will need to identify:

- How the breach occurred
- When it happened and how long it was happening for
- What categories of data were taken
- The number of records/subjects affected
- How you have mitigated the breach

Consent

Burden of truth has been reversed. Consent must be given by specific action and verifiable. Freely given, specific, informed, unambiguous and separate from other terms. Should be as easy to withdraw as it was to give. This builds trust and engagement, enhances your reputation. Must be granular and prominent, not hidden away or in lengthy documents. Silence, inactivity or pre-ticked boxes no longer constitute consent. If your lawful basis for processing is based on inferred consent it cannot be used. Avoid making consent a precondition of a service.

Consent

Must be in a language a child will understand. Age verification may be required. Age of a child is currently under 16. Verified consent must be provided for a child by a parent or guardian. Name any Data Processors who will rely on the consent. Make it as easy for people to withdraw consent and tell them how to do so. Keep evidence of consent - who gave it, how and when, and what they were told. Keep consent under review and refresh it if anything changes. Be careful about sending out blanket consent requests. If your reason for sending is due to your questionable lawful basis, you are likely breaching PECR. Non-response prejudices your right to claim legitimate interest.

Transferring data outside of the EEA

Significant restrictions on personal data being transferred outside the EEA. Must be stored only in specific 'third countries' that provide 'adequacy of protection'. Andorra, Argentina, Canada, Faroe Islands, Guernsey, IoM, Israel, Jersey, New Zealand, Switzerland, Uruguay. If in the US, they (at the very least) need to be part of the 'Privacy Shield' scheme. If they are not a member, they should not be used. Privacy Shield may fail in a similar way to Safe Harbour. Other countries can be used, however you must confirm 'adequacy of protection'. Carry out an assessment of adequacy. No different to EU Data Processors, ensure the recipient will process the data in a compliant way. Use EC approved model contractual clauses. Get your Binding Corporate Rules approved by the ICO

Impact assessment

Carry out an Impact Assessment on all your datasets. Required as it provides the foundation for building trust and demonstrating compliance. Identify all places where personal data is gathered, processed and stored. Audit each dataset to ensure you understand who is responsible for it and if you are the Controller, joint Controller or Processor.
The categories of data within it (personal, sensitive, special category). Where it came from and who it is shared with. The lawful basis upon which you are processing it. What is stored, where it is stored, is it correct and complete, how it is secured and when and where is it backed up. Who has access to it, why and how is that access logged. How long it is retained and how is it deleted

Legal issues

Ensure you have contracts with all your Data Processors. Contract must imply the same data protection obligations as if they were the Controller. Agree who will incur additional costs or if this is part of the service. Ensure they understand where the liabilities stand should they have a breach. Ensure Processors require prior written consent before sub-contracting processing, and require a minimum notice period so that you have time to object.
Make insurance a pre-requisite on Processors to cover situations where they can't pay, though you must take out cover for your own liabilities and to cover where they can't pay. Update employment contracts to include employee rights under GDPR. Update handbook policies for privacy, IT usage, email and information security

Privacy policies

Update your privacy notices on your websites, forms and contracts. Identify who the Data Controller is. The 3rd party Data Processors that will receive the data. Make subjects aware of the risks, rules, safeguards. Clearly state their rights and how to exercise them. Identify the lawful basis upon which data is processed. State the time period data will be held and procedure for how it will then be deleted. Provide contact details for your DPO and who SARs should be addressed to. Indicate their right to complain to the ICO together with the ICO's contact details

IT issues

Implement 'proportionate' measures to reduce the risk of data breaches. Encrypt your data 'at rest' and in transit. If you do, it's your 'get-out of-jail-free' card. Ensure only the right people have access to the minimum of data. Introduce access logging to assist with breach detection and reporting. Ensure systems can comply with Subjects' various rights. Implement consent appropriately on your websites.

Ensure you can identify who gave it, how and when, and what they consented to. You may need automated systems to enable you to respond to SARs

Appoint a Data Protection Officer

A DPO acts as your compliance lead

All public bodies and large-scale processors are required to appoint a DPO

Must have expert knowledge of data protection law. Needs to be able to perform their duties in an independent manner. Able to exercise their functions free of undue influence or pressure from the organisation. Need to avoid conflict of interest. Must be provided with sufficient resources.

Cannot be dismissed merely for performing their tasks. Must report directly to the "highest management level". A Data Protection Officer needs managing, ongoing training, holiday cover and value lost if they leave.

Be ready

25th of May 2018.

Start now – Set a budget

Understand the impact

Assign the necessary resources

Train your staff and increase awareness

Make the necessary changes

Implement new systems

Improve your processes

robert.masson@dpocentre.com
0203 797 1289
07802 455109

Recommended: that Council delegate the drafting of policy and procedures regarding the Council's responsibilities under the new General Data Protect Regulations to the Policy Review Working Group for consideration at an early future meeting of the Parish Council.

Peter Whitehouse
Parish Clerk