



The Church of England  
in Essex and East London  
Diocese of Chelmsford

# **The General Data Protection Regulation/ UK Data Protection Act 2018**

8 September 2018

# The aim of today

- Dispel myths
- Help you to understand what is required
  - The law is not always black and white
- Explain what the General Data Protection Regulation (“GDPR”) means in practice
  - Electoral Roll
  - Baptism, Marriage, Funeral
  - Pastoral care
  - Prayer list
  - Websites
  - Gift Aid
  - Rotas/parish magazines
  - CCTV
  - Employment context
  - Other
- Explain what the Privacy and Electronic Communications Regulations (“PECR”) require
- Give you the opportunity to ask any questions
  - Please remember there is no such thing as a stupid question!
- Explain what resources are available

# Background

- The GDPR came into effect on 25 May 2018
- The UK Data Protection Act 2018 received Royal Assent on 23 May 2018
- The GDPR/DPA only concerns the processing of personal data, i.e. data collected, generated or derived from/in relation to a data subject (living individual)
  - governs all aspects of the processing of personal data, from collection to destruction
- Changes
  - Many requirements are the same or very similar to the law today
  - New administrative obligations
  - Increased rights for data subjects
  - Potential for significant fines (up to €20M)
- The UK regulator is the Information Commissioner

# Key definitions

- **Data Subject** – an identified or identifiable individual
- **Personal data** – information relating to an data subject [individual], who can be identified directly or indirectly from that information
- **Special (sensitive) categories of personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation.
- **Processing** – anything you do with personal data!
- **Controller** – determines the purpose of the processing and how it will be done
- **Processor** – processes personal data on behalf of the controller

# The Data Protection Principles

Largely the same as under current law and must be applied to all personal data processing:

1. **Lawful, fair and transparent** – the processing must meet one of a set of prescribed conditions, the processing must be considered fair, and data subjects must be made aware of the purposes for which their personal data will be processed and who it will be disclosed to
2. **Purpose limitation** - collected for a specified, explicit and legitimate purpose, and not processed for any other purpose that is incompatible with that purpose
  - Electoral roll
3. **Minimisation** - adequate, relevant and limited to what is necessary for the purpose processed
4. **Accuracy** - accurate and where necessary kept up to date
5. **Storage limitation** – not kept longer than necessary for the purpose processed
6. **Integrity and confidentiality** – appropriate security measures must be in place to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage.

Compliance with the principles must be able to be demonstrated – this is known as accountability

# Transparency

Data Subjects must be provided with the following information:

- The contact details of the data protection officer if one is appointed
- An explanation of the legal basis for the processing
- If legitimate interests is relied upon, what those legitimate interests are
- Whether the personal data will be transferred overseas
- How long personal data will be retained
- Details of their rights
- The right to complain to the ICO
- Whether the provision of personal data is mandatory
- The right to opt out of marketing

There are different ways of doing this – it does not always have to be through the provision of a separate privacy notice

# Processing conditions

For the processing to be considered lawful, one of the following conditions must be met:

- Consent
  - Not always necessary!
  - Cannot be an opt out box
  - If relied upon, must be able to demonstrate how obtained
  - Must be a true choice and easy to withdraw
- Performance of a contract to which the data subject is party
- Compliance with a legal obligation
- Necessary to protect the vital interests of an data subject
- Public interest
- Legitimate interests as long as the rights and freedoms of the data subject are not overridden

The processing condition is important as in some cases this determines what rights a data subject has.

# Processing conditions – special categories of personal data

If special categories of personal data are processed, one of the following conditions must be met:

- Explicit consent
- Exercising rights in the field of employment and social security and social protection law
- Compliance with a legal obligation
- Necessary to protect the vital interests of a data subject where the data subject is physically or legally incapable of giving consent
- **Legitimate activity with appropriate safeguards by a foundation, association or any other not-for-profit body with a ... philosophical, religious ... aim if the processing relates to the members or former members or to people who have regular contact with it in connection with its purposes**
- The personal data is made public by the data subject



## Processing conditions – special categories continued

- Establishment, exercise or defence of legal claims
- Public interest
- Medicine, health, social care...by a professional under an obligation of secrecy
- Public interest in the area of public health
- Archiving in the public interest, scientific or historical research

Other conditions introduced under the UK DPA 2018

# How the principles and processing conditions work in practice

Is the processing fair



Apply all of the principles



Meet one of the processing conditions



If special category of personal data, meet one of the special category processing conditions

## **Record keeping and demonstrating accountability**

- A record must be kept of all personal data processing activities including who is processing what personal data, for what purpose, how, where and who it may be disclosed to
- Compliance with the privacy principles must also be able to be demonstrated

# Personal data breach reporting

- A personal data breach occurs when there 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.
- Unless the personal data breach will not result in a risk to a data subject, the UK Information Commissioner must be notified 'without undue delay' and where feasible within 72 hours. Notifications made after 72 hours must be accompanied by a justification for the delay in reporting.
- If there is a chance of there being a high risk of harm to data subjects, they must also be notified. There is a risk of harm if any of the following are likely to occur:
  - Threat to personal safety
  - Discrimination
  - Identity fraud
  - Financial loss
  - Humiliation or loss of dignity, damage to reputation or relationship
  - Loss of business and employment opportunities

# Personal data breach reporting continued

- If one of the following conditions is met, a data subject does not have to be notified of a personal data breach:
  - Technical and organisational measures were taken to protect the personal data prior to the breach, for example encryption on a laptop that would mean someone not authorised to access it would not be able to
  - Following a breach steps have been taken to ensure the risk is no longer likely to materialise, for example action taken against the unauthorised parties likely to access it before they were able to do anything with it
  - Notifying would involve disproportionate effort in which case a public communication must be made

# Third Party Processors

- As with current law, the GDPR requires that where processing is going to be carried out by a third party processor (“processor”) the controller must:
  - conduct due diligence on the third party to ensure there are appropriate technical and organisational measures in place to ensure the requirements of the GDPR and the protection of the rights of the data subject will be met;
  - put appropriate contractual clauses in place to govern the protection of the Personal Data as well as limiting how the personal data can be processed; and
  - take steps throughout the duration of the contract to ensure the third party is in compliance with those terms.
- Under the GDPR data subjects can take action against a processor as well as the controller

# Data Subjects' rights

- Right of access to personal data (Data Subject Access Request (“DSAR”))

A data subject is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the personal data; and
- given details of the source of the data (where this is available).

The response must be provided within one month (there are some exceptions to this but unlikely to apply).

- Right to erasure

The right to erasure has widely been wrongly reported as a general ‘right to be forgotten’. The right is a right to the erasure of personal data:

- When no longer necessary in relation to the purpose of collection
- When consent is withdrawn but only if there is no other legal ground to justify the processing

- Right to restriction of processing

An data subject has the right to the restriction of processing of personal data in some circumstances.

## Data Subjects' rights continued

- Right to data portability

Not intended to apply to the Church

- Right to object

A data subject has the right to object to:

- processing based on legitimate interests, including profiling
- direct marketing and profiling for the purposes of direct marketing

- Automated decision making

- data subjects have the right not to be subject to decisions based solely on automated processing, including profiling in most circumstances.

Unlikely to apply to the Church



# Criminal Convictions and Offences

- Personal data relating to criminal convictions and offences and convictions can only be processed under the control of an official authority (i.e. DBS) or when authorised by law.
- All applicants for a DBS check should be made aware of the DBS Code of Practice for Registered Persons and provided with a copy on request.
- Registered Persons must have a written policy on the secure handling of information provided by DBS, electronically or otherwise, and make it available to data subjects at the point of requesting them to complete a DBS application form or asking consent to use their information to access any service DBS provides.
- Have a written policy on the suitability of ex-offenders for employment in relevant positions. This should be available upon request to potential applicants.
- Notify all potential applicants of the potential effect of a criminal record history on the recruitment and selection process and any recruitment decision.

# Marketing

- The GDPR/DPA gives data subjects the right to opt out of receiving direct marketing.
- Direct marketing from a privacy perspective means the communication by any means of any advertising material directed to particular data subjects. Material intending to promote the aims or ideals of an organisation (including not-for-profit organisations), any particular service or event, even where it may be of benefit to the data subject, also falls within the definition of marketing.
- Non direct marketing occurs if, for example, a leaflet detailing Christmas service details, is put in the mailbox of every home in a particular area or inserted into a newspaper or magazine.
- The Privacy and Electronic Communications Regulations (“PECR”), which sit alongside the GDPR/DPA, also need to be taken into consideration:
  - Opt in consent needed for electronic marketing, i.e. email or SMS
  - Each electronic message must enable easy opt out of receiving anything further
- Prospect lists must be screened against the preference service lists

# Marketing

Data protection | Privacy and Electronic

## At-a-glance guide to the marketing rules

Method of communication	Individual consumers (plus sole traders and partnerships)	Business-to-business (companies and corporate bodies)
Live calls	<ul style="list-style-type: none"><li><input type="checkbox"/> Screen against the Telephone Preference Service (TPS)</li><li><input type="checkbox"/> Can opt out</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Screen against the Corporate Telephone Preference Service (CTPS)</li><li><input type="checkbox"/> Can opt out</li></ul>
Recorded calls	<ul style="list-style-type: none"><li><input type="checkbox"/> Consumer must have given caller specific consent to make recorded marketing calls.</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Consumer must have given caller specific consent to make recorded marketing calls.</li></ul>
Emails or texts	<ul style="list-style-type: none"><li><input type="checkbox"/> Consumer must have given sender specific consent to send marketing emails/texts.</li><li><input type="checkbox"/> Or soft opt-in (previous customer, our own similar product, had a chance to opt out)</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Can email or text corporate bodies</li><li><input type="checkbox"/> Good practice to offer opt out</li><li><input type="checkbox"/> Individual employees can opt out</li></ul>
Faxes	<ul style="list-style-type: none"><li><input type="checkbox"/> Consumer must have given sender specific consent to send marketing faxes</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Screen against the Fax Preference Service (FPS)</li><li><input type="checkbox"/> Can opt out</li></ul>
Mail	<ul style="list-style-type: none"><li><input type="checkbox"/> Name and address obtained fairly</li><li><input type="checkbox"/> Can opt out</li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Can mail corporate bodies</li><li><input type="checkbox"/> Individual employees can opt out</li></ul>

# Privacy Impact Assessments

A Privacy Impact Assessment (“PIA”) has to be completed for proposed high risk processing.

A PIA is an assessment of how the proposed activity will comply with the privacy principles

# Websites

## Cookies

Cookies are small data files which are placed a device when visiting certain parts of a website or when clicking on online advertisements.

- **Strictly necessary cookies** are required for the operation of a website by:
  - allowing web servers to determine whether the cookies setting on the device web browser have been enabled or disabled. This allows the site to know whether data can be collected from the visitors web browser.
  - temporarily allowing information to be carried between pages of a website to avoid having to re-enter that information.
  - temporarily identifying a device after logging in to a secure page on a website so that the web server can maintain a dialogue with the visitors web browser in order for the visito to carry out certain activities.
- **Analytical/performance cookies** are used to help improve websites by tracking visits to a website and recognising a web browser of repeat visitors so that statistics can be gathered on new and repeat visitors to evaluate website effectiveness.
- **Functionality cookies** are used to recognise visitors returning to a website. This enables a website to:
  - remember the choices made by the visitor (such as your user name, language and region) so it does not have to be re-entered when revisiting a website
  - personalise website content
- **Targeting/advertising cookies** record visits to a website, responses to online advertisements, track pages visited and the website links that have been followed. This information is used to:
  - make websites more relevant to the visitors interests based on past visits to the website
  - tailor online advertisements or offers on third party websites to those which are most likely to be of interest to the visitor
  - evaluate the effectiveness of online marketing and advertising campaigns.

# Websites continued

## Why do cookies matter?

- If cookies are used, a cookie policy/statement is required on the website.
- PECR requires that consent is obtained from visitors to a website if cookies or similar technology is used. Consent can be implied, but must be knowingly given.
  - This is done by displaying a message when first logging onto a site, for example:

This site uses cookies to provide you with the best possible online experience. By using this site, you agree that we may store and access cookies on your device. Find out more about our use of cookies ([link to cookie policy](#))

## Contact us pages:

- Ideally ensure the submission is secure (https)
- If not, advise people not to submit anything confidential

**Ensure personal data published on the website, i.e. photographs and contact details, meets the principles and processing conditions**

# ICO Fees

Exemptions apply if the processing is only for one or more of the following:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Not-for-profit purposes
- Personal, family or household affairs
- Maintaining a public register
- Judicial functions
- Processing personal information without an automated system such as a computer

A specific exemption applies to bodies or associations that are not established or conducted for profit. However, the exemption applies only if:

- The processing of personal data is for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are members of the body or association or have regular contact with it
- Information is only held about individuals whose data needs to be processed for this exempt purpose
- the personal data processed is restricted to personal information that is necessary for this exempt purpose

Exemptions may not apply - pastoral care is called out as not exempt. The fee is £40

ICO fee assessment tool can be found at:

- <https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/>

## Other issues

- Parishes do not need to appoint a Data Protection Officer under the GDPR but good practice to have someone designated as responsible.
- The GDPR indicates the age of consent for children in relation to on-line activities is 16. The UK DPA 2018 has amended this to 13.



# Resources

- Parish Resources

<http://www.parishresources.org.uk/gdpr/>

- ICO Guide to the GDPR

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>

- ICO Employment Practices Code

[https://ico.org.uk/media/for-organisations/documents/1064/the\\_employment\\_practices\\_code.pdf](https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf)

- ICO Direct Marketing

<https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf>

- ICO CCTV Code of Practice

<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

- Subject Access Code of Practice

<https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf>

- Practical Guide to Security for small business

[https://ico.org.uk/media/for-organisations/documents/1575/it\\_security\\_practical\\_guide.pdf](https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf)

Thank you

Any questions?