THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

General Data Protection Regulation (GDPR) and Data Protection

Key messages for the Church of England

NCIs GDPR working group
December 2017

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Contents

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

What is personal data?

Personal data is defined as:

> Any information about a living individual which is capable of identifying that individual.

Sensitive personal data is defined as:

> Any information relating to an individual's racial or ethnic origin, political opinions, ***religious beliefs***, trade union membership, physical or mental health or condition, sexual life, alleged or actual criminal activity and criminal record.

(Under GDPR sensitive personal data is referred to as "special categories of personal data")

A Quick reminder - What is personal data?
This often causes confusion – often people think it is simply a name and address.

The law defines **personal data** as - Any information about a living individual which is capable of identifying that individual.

The law additionally defines an extra data set which need more and better protection - Sensitive personal data

And that is - Any information relating to an individual's racial or ethnic origin, political opinions, ***religious beliefs***, trade union membership, physical or mental health or condition, sexual life, alleged or actual criminal activity and criminal record.
It doesn't matter if that data is already in the public domain – you still have to comply with the DPA in the way in which you collect, use and store it.

GDPR stretches this further and for example says that an IP address can be personal data – for the less technical among us (and that includes me) an IP address is Internet Protocol address and it is used to identify computers communicating via the internet. So if you've ever wondered why the ads around web pages you view are so closely related to what you recently searched for (a new sofa, flights to Italy….). Of course they may be related to what another family member has been searching for….

In summary – the definition is far broader than “name and address”.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

What is Data Protection?

Data Protection is about **avoiding harm** to **individuals** by misusing or mismanaging their personal data.

So if you collect, use, or store personal data then the Data Protection Act applies to you. It sets out eight principles you have to adhere to, which include:

- Only collect information for specific purposes and don't then use it for other purposes
- Only collect what you need for the specific purpose
- Keep it accurate and up to date; and safe and secure
- Process information lawfully and allow subject access in line with the Act.

So, a quick re-cap of the Data Protection Act –
Data Protection is about preventing harm to individuals by misusing or failing to look after their personal data. It applies to ALL organisations in the UK through the Data Protection Act (DPA).
So, if you collect, use, store personal data then the law applies to you.

There are eight governing principles but I have summarised them here as:
Only collect personal data for specific purposes and then only use it for those purposes. Collect just the data you need for the purpose and keep it accurate and up to date; and don't keep it for longer than is necessary for the completion of the purpose for which it was collected. You will need consent from data subjects to process their data. You will also have to register with the Information Commissioner's Office (ICO) as a data controller – whether you know it or not you already have ! Typically dioceses have registered in the name of the DBF; Bishops in the name of the Bishop in his or her corporate capacity and Cathedrals, the Dean and Chapter. This is a public register – you can search it via the ICO
Keep the data securely whether paper or electronic. Avoid storing it outside the European Economic Area – might be an issue if your electronic data is in the cloud.

Finally, be aware of the rights of subjects to access certain data you hold about them through a Subject Access Request (SAR). Note that this does NOT necessarily mean that

they can see everything you hold about them – seek advice from your registrar whenever you get a SAR.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

What is GDPR?

It is the **General Data Protection Regulation**, which supersedes the Data Protection Act on 25th May 2018. The key changes from the current law are to strengthen rights of individuals and place more obligations on organisations in looking after personal data.

In order to comply with the new law:

- You must have a legitimate reason for processing data – this will cover much processing we undertake (see later slide)
- Consent must be freely and unambiguously given and can be just as easily withdrawn
- Data Processing activities must start with "privacy by design and default".

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

What is GDPR? …continued

- Subject Access Requests – will include how you process and share data not just what you hold and you'll have less time to respond
- Subjects can request data deletion – "the right to be forgotten", though only in certain circumstances
- There will be mandatory breach reporting
- Data processors will be held liable
- You must be able to demonstrate compliance with GDPR
- While the ICO say it is a last resort, the potential fines are much greater than at present – up to 4% of annual global turnover or €20m
- And finally – it's happening regardless of Brexit!

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

GDPR Principles

- **Lawfulness, fairness and transparency** – as with Data Protection
- **Purpose limitation** – only collect for specific purposes and then don't use it for other purposes
- **Data minimisation** – only collect the data you need for the purpose you are using it
- **Accuracy** – as now, keep it up to date!
- **Storage limitation** – don't keep it for longer than you need to fulfil the purpose
- **Integrity and confidentiality** – keep it safe and secure e.g. encrypted if on a laptop or mobile phone.
- **Accountability** – you must be able to prove you have complied with the above.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

GDPR / Data Protection Terminology

- The **data controller** is the person or organisation who determines the how and what of data processing.
- The **data subject** is the person about whom personal data is being processed.
- A **data processor** is the person or organisation who takes an action with the personal data you control – this might be a 3rd party acting on your behalf.
- **Processing** is anything done with/to personal data, including storing it.
- The **Data Protection Officer (DPO)** is a specific role which will be a legal requirement for many organisations including large church bodies such as NCIs or dioceses.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Data Protection Officers

- The law requires that in certain circumstances organisations must have a named Data Protection Officer (DPO). One of these is where there is large scale processing of "special categories of personal data". This will affect larger Church organisation such as dioceses and the NCIs. The NCIs will share a DPO.
- The DPO has an education and compliance role regarding GDPR and is the first point of contact for the wider world. They must report to a senior level in the organisation and be independent – so similar to Internal Audit.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Subject Access Requests

- These will still need to be carried out by the people who do them now, so are not part of being the DPO.
- So that means if at present you don't deal with these but pass them onto a named colleague then **nothing changes.**
- However, they have to be completed in a month rather than 40 days so pass them on promptly.
- The £10 charge is abolished.
- If you do deal with these then clear guidelines will be provided before May 2018 on how it changes under GDPR and what you'll need to do differently.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Can I still process personal data? Do I need consent?

- GDPR (and DPA) are all about making sure data processing and sharing is done properly – they aren't there to prevent legitimate data sharing, so there is a lot you can do without consent. For example, you can process personal data **without** consent where it is necessary:
  - For the performance of a contract
  - For compliance with a legal obligation
  - To protect the vital interests of the data subject or another person
  - In the exercise of official authority or in the public interest
  - For the purposes of legitimate interests you are undertaking
- ONLY if NONE of the above apply do you need consent.

While there are some caveats about some of the above the core message is that there is a lot you can do WITHOUT consent.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

What are the NCIs doing?

- Action Plan being prepared – what we need to do
- GDPR Project Group formed – making sure we do it
- NCIs Gateway pages with information
- Parish guidance is already available: **http://www.parishresources.org.uk/gdpr/**
- Data Sharing protocols being created to support our data sharing across the Church of England – Early 2018
- Key messages factsheet for the wider church
- All guidance and training will be designed to be adaptable to a wide range of church settings.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

What do I and my team need to do?

- First of all **don't panic!** If you are complying with the Data Protection Act then you are well on the way to GDPR compliance
- Secondly, dust off your departmental Information Directory (which was compiled a few years ago and lists all the sensitive and confidential data you hold) and check that it is up to date
- The Records Management team will be in touch in the new year to start working through what you and your team will need to do to prepare for GDPR compliance.

THE CHURCH OF ENGLAND
NATIONAL CHURCH INSTITUTIONS

Where to get more information

- NCIs' staff intranet: https://www.ncisgateway.com/knowledge/425/gdpr/
- Information Commissioner's Office website: www.ico.gov.uk
- Comments / queries / feedback: gdpr@churchofengland.org