



Writing a Privacy Notice (GDPR)

A Guide for Parishes

What's all this about?

Data Protection in the UK is changing in May 2018 and the new law gives individuals (you and me) more rights over how information about them is stored and used by organisations (a PCC or a Diocese for example). In particular, organisations have to tell individuals what they are doing with the information they are storing and using.

Does it apply to me and my organisation?

If you work or volunteer in an organisation that holds information about people (e.g. their name or address or their gift aid donation details) then this DOES apply to you. In practice, most church organisations from PCCs all the way through to the Archbishops will be storing and using some personal information. So, yes it will almost certainly apply. More guidance for PCCs can be found at www.parishresources.org.uk/gdpr

What's in this guide?

What follows is in four parts: a couple of pages explaining the jargon and what sort of things you are going to have to tell people in what is known as a privacy notice; then a template privacy notice in which we've tried to fill in as much as we can for you and suggested where things can be deleted; a ready to use consent form in case you need one, with advice throughout about using them both. Then finally a completed example of how these both might look for a parish.

What do I have to do?

Read through the guidance and decide which bits apply to your organisation. We've colour coded the most likely green and least likely red to help. You can fill in the information specific to your organisation and delete all the bits that don't apply. Once you've got a final version ready to send then you need to send it to all of the people that you hold data about. Keep a record of who you sent it to, when, and how. If you are sending consent forms then you need to keep them all as they are returned.

When do I have to do it?

By May 2018 – so while you've got quite a bit of time, it's a good idea to get started now and not leave it all to the last minute.

DATA PROTECTION PRIVACY NOTICE AND CONSENT FORM GUIDANCE

This guidance covers privacy notices and consent forms; explains what you need to do; and provides templates and a “typical parish” example for you to use.

When you collect, use, store and manage personal data then the new General Data Protection Regulation (GDPR) requires that you tell individuals what you are doing with the information. The GDPR sets out the information that you should supply to individuals and when.

What you have to tell people depends on whether or not you obtained the personal data direct from them or got it from somewhere or someone else. The information table below sets out what you’ve got to supply.

Under the GDPR, the information you supply about the processing of personal data **must** be: -

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

Explaining the jargon used in the Table below:

Personal data is information about a living individual which is capable of identifying that individual.

Processing is anything done with/to personal data, including storing it.

The **data subject** is the person about whom personal data are processed.

The **data controller** is the person or organisation who determines the how and what of data processing, in a parish usually the incumbent or PCC.

Information Table

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the data controller and where applicable the controller’s representative and the data protection officer	Yes	Yes
Purpose of the processing and the legal basis for the processing	Yes	Yes
The legitimate interests of the data controller or third party (where applicable)	Yes	Yes
Categories of personal data	No	Yes
Any recipients or categories of recipients of the personal data	Yes	Yes
Details of international data transfers	Yes	Yes
Retention period or criteria used for determining the retention period	Yes	Yes
The various rights of the data subject	Yes	Yes
The right to withdraw consent at any time, where relevant	Yes	Yes
The right to lodge a complaint with a supervisory authority	Yes	Yes

The source from where the personal data originates and whether it came from publicly accessible sources	No	Yes
Whether the provision of personal data is part of a statutory/legal or contractual requirement or obligation, and possible consequences of failing to provide the personal data	Yes	No
The existence of automated decision making, including profiling and information about how decisions are made, the significance and consequences	Yes	Yes

When should the information be provided?

If the personal data is obtained directly from the individual, then you've got to tell them at the time you collect the data.

If the personal data is not obtained directly from the individual, then you need to tell them within a reasonable time (i.e. within one month). If you are using that data to communicate with the individual then you should tell them when you first communicate with them. If you are passing the data onto someone else you must tell the individual BEFORE you pass it to anyone else.

DATA PRIVACY NOTICE

[Insert name of relevant person/body/organisation]

Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by *[the General Data Protection Regulation 2016/679 (the "GDPR")¹]*.

Who are we?

[Insert name of relevant person/body/organisation] is the data controller (contact details below). This means it decides how your personal data is processed and for what purposes.

How do we process your personal data?

[Insert name of data controller] complies with its obligations under *[the GDPR]* by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes: -

¹ At the time of going to press the new Data Protection Bill, which incorporates the GDPR into national law, has started its journey through parliament. The final form of this legislation is not yet known, we have therefore referred to the GDPR as the relevant legislation.

The GDPR: A Basic Guide to Data Processing for Parishes

[Insert relevant details – The notice must include a description of all the purposes for which the personal data will be processed. It is advisable to keep the description of the purposes as broad as possible, whilst ensuring that it is accurate and not in any way misleading. If a purpose is missed out, the personal data may not, in most cases, be used for that purpose without reissuing the data protection notice setting out the new purpose, processing condition and other relevant information. That said, this does not mean that you can include in the notice every possible purpose, the purposes included must be reasonably foreseeable].

Examples of the relevant purposes might be as follows: -

- For members of the clergy - To provide pastoral care to my parishioners;
- For Diocesan bodies –
 - To enable us to provide a voluntary service for the benefit of the public as specified in our constitution;
 - To administer membership records;
 - To fundraise and promote the interests of the charity;
 - To manage our employees and volunteers;
 - To maintain our own accounts and records.
 - [Our processing also includes the use of CCTV systems for the prevention of crime].
- For PCCs –
 - To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;
 - To administer membership records;
 - To fundraise and promote the interests of the charity;
 - To manage our employees and volunteers;
 - To maintain our own accounts and records.

Other examples of purposes which could be applicable are: -

- To operate the [*insert name of relevant body*] web site and deliver the services that individuals have requested.
- To inform individuals of news, events, activities or services running at [*insert name of relevant body/church*].
- To share your contact details with the diocesan office so they can keep you informed about news, events, activities and services that will be occurring in the diocese and which are relevant to the role you are undertaking.
- To process gift aid applications.
- To contact individuals via surveys to conduct research about their opinions of current services or of potential new services that may be offered.

[Please note that these lists are not exhaustive and you may process personal data for other purposes, which will need to be recorded. Remember, at the heart of this is ensuring that individuals are aware of exactly what you are going to do with their personal data and giving them the opportunity to consent where necessary]

What is the legal basis for processing your personal data?

The GDPR: A Basic Guide to Data Processing for Parishes

These fall under either article 6 or article 9 – dealt with separately below.

[You will need to insert here the relevant processing condition contained in Article 6 of the GDPR – e.g. consent, legitimate interests of the data controller etc. Please click on the box that relates to the relevant processing condition and please insert any relevant details where required. Irrelevant processing conditions can be deleted. For ease of reference, the processing conditions have been colour coded as follows: - “Green” means most likely to be a relevant processing condition; “Orange” means may be a relevant processing condition and “Red” means unlikely to be a relevant processing condition].

Article 6 processing

- Consent of the data subject;**

[Where the processing is based on the consent of the data subject, you will need to provide a link to the “Consent Form” at the end of this notice].

- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract** *[If so, insert details of the contract];*

- Processing is necessary for compliance with a legal obligation;**

[You will need to provide details of whether there is a statutory or contractual requirement to provide the data and if so, the consequences of not supplying the data].

- Processing is necessary to protect the vital interests of a data subject or another person;**

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;**

- Processing is necessary for the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.** *[Where the processing is based on the legitimate interests of the data controller, you will need to set out what are the legitimate interests].*

[If you are processing special category personal data (i.e. sensitive personal data), as well as satisfying one of the processing conditions set out in Article 6 (above), you will also need to satisfy one of the processing conditions set out in Article 9 (below). You should note that the same colour coding as detailed above applies. Personal data which reveals religious belief is classed as sensitive personal data under the GDPR].

Article 9 Processing

- Explicit consent of the data subject** *[link to “Consent Form” as above];*

[Use this for example, to be able to tell people about events, news, services]

- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;**

- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;**

- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided: -**

- the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
- there is no disclosure to a third party without consent.

[This clause allows you to collect and process data without consent]

- Processing relates to personal data manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest on the basis of EU or Member State law;
- Processing is necessary for reasons of preventative or occupational medicine, for assessing the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional;
- Processing is necessary for the reasons of public interest in the area of public health;
- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

[Where the personal data are collected direct from the data subject, the data subject must be informed whether he or she is obliged to provide the personal data and the consequences, if he/she does not provide the data].

[The wording to the GDPR including full details of the processing conditions contained in Article 6 and Article 9 can be found here - <https://gdpr-info.eu/>]

Sharing your personal data

Your personal data will be treated as strictly confidential, and will be shared only with *[insert the recipients or categories of recipients of any personal data]*. We will only share your data with third parties outside of the parish with your consent.

How long do we keep your personal data²?

*[We keep your personal data for no longer than reasonably necessary for a period of *[insert relevant period]* in order to *[insert sufficient reason for retaining personal data – (“just in case” it might come in useful one day, will not be a sufficient reason)]*. Examples could be: - in case of any legal claims/complaints; for safeguarding purposes etc.].*

OR

[If you cannot state a specific period, you will need to set out the criteria that you use in order to determine a retention period].

² Details about retention periods can currently be found in the Record Management Guides located on the Church of England website at: - <https://www.churchofengland.org/about-us/structure/churchcommissioners/administration/librariesandarchives/recordsmanagementguides.aspx>

The GDPR: A Basic Guide to Data Processing for Parishes

[We keep your personal data for no longer than reasonably necessary and we only retain your data for the following purposes and use the following criteria to determine how long to retain your personal data *[insert relevant purposes and criteria for retention]*].

Your rights and your personal data

Unless subject to an exemption *[under the GDPR]*, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which the *[insert name of data controller]* holds about you;
- The right to request that the *[data controller]* corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for *[data controller]* to retain such data;
- *[The right to withdraw your consent to the processing at any time] [Only insert if consent is relied upon as a processing condition];*
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable) *[Only applies where the processing is based on consent or is necessary for the performance of a contract with the data subject and in either case the data controller processes the data by automated means]*.
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable) *[Only applies where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics]*
- The right to lodge a complaint with the Information Commissioners Office.

[Transfer of Data Abroad

If the personal data is to be transferred to countries or territories outside the EU you must include details of how the data will be protected, together with details of how to obtain copies of the relevant safeguards].

[Automated Decision Making

You will need to provide details of any automated decision making, together with information about the logic involved and the significance and consequences of the processing for the individual].

Further processing

If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Contact Details

To exercise all relevant rights, queries of complaints please in the first instance contact the PCC Secretary / Parish Administrator at *[insert contact details]*.

The GDPR: A Basic Guide to Data Processing for Parishes

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

[The paragraph entitled "Consent" below can be adapted and used where consent is to be relied upon in order to process the personal data]

[Consent

By signing this form you are confirming that you have read this Data Protection Notice and that you are consenting to *[insert name of the Data Controller]* holding and processing your personal data for the following purposes (please tick the boxes where you are happy to grant consent): -

Name:.....

Address.....

.....

Telephone.....

Email address.....

[Insert relevant purposes where you will be relying on consent to process the personal data, for example: -

[To keep you informed about news, events, activities and services;

To contact you with surveys about current events;

To share your contact details with the diocesan office so they can keep you informed about news and events, activities and services that will be occurring in the diocese and which are directly relevant to the role you are undertaking;

All of the above.]

By email [] by text [] by post [] by phone []

You can grant consent to all the purposes; one of the purposes or none of the purposes. Where you do not grant consent we will not be able to use your personal data *[you can insert further details here about what will happen if someone does not consent to processing, for example, they won't be able to receive papers, updates etc.]*, except in certain limited situations, such as where required to do so by law or to protect members of the public from serious harm.

If you do grant consent, please note you can withdraw your consent to all or any one of the above purposes at any time by contacting *[insert contact email address or link to paragraph containing contact details]*. Please note that all processing of your personal data will cease once you have withdrawn consent but this will not affect any personal data that has already been processed prior to this point.]

.....
SIGNED

.....
DATED

The GDPR: A Basic Guide to Data Processing for Parishes

[insert name and registered charity number of the PCC if applicable]

[Please note – if the personal data is not obtained directly from the data subject, the data controller will need to provide the data subject with the following additional items of information within 1 month of having received their personal data: -

- *The categories of the personal data you are processing; and*
- *The source from where the personal data originates and whether it came from publicly accessible sources]*