St Saviour

ST ALBANS

Introduction to the

General Data Protection Regulations

On the 25th May the UK's Data Protection Act 1998 (DPA1998) will be replaced by the European Union's General Data Protection Regulation (GDPR). The new regulation is aimed at making organisations more accountable and transparent with regard to the data that they hold on individuals. The provisions in the GDPR sets out what information should be supplied to these individuals and when, and gives those individuals greater control over the use of their personal data. The GDPR will apply to all organisations – regardless of size - which collect, use, store and manage personal data about individuals and as such will apply to the PCC. However it should be emphasised that the GDPR has been developed to meet a wide range of Data Protection scenarios and practices used by a wide range of organisations. It is essentially a "catch-all" measure and there are issues covers in the Regulation which will be of significance to the large and complex organisation which will be of little relevance to small organisations and charities such as the PCC.

With the possibility that the UK will be leaving the EU through the current Brexit negotiations, the UK Government has prepared a Draft Data Protection Bill which is currently going through Parliament. In effect this mirrors the provisions in the GDPR but with some additions. One change that the draft Bill introduces is that the age at which children can give their own consent without the need for parental consent, is lowered from the current sixteen years to thirteen. The GDPR allows Member States to introduce such a change.

Understanding the language

Inevitably in a legal document such as the GDPR, or a Statute, there will be some terms or expressions used which have a particular meaning and which need to be understood so that that particular piece of legislation can be used correctly and effectively. The main ones in the DPA 1998 and the GDPR which need to be understood are:

The "**Data Subject"** is the particular living person(s) whose Personal Data is being collected, held and used.

A **"Special Subject"** is someone whose data, if processed, would reveal , amongst other aspects, their racial or ethnic origin, political opinions, or their

religious or philosophical beliefs. In these cases special measures must be taken.

"**Personal data"** means any information about a living individual which can be used to identify that individual. It applies to any data that is being held either on paper or electronically and includes information such as name, date of birth, address, telephone numbers and e-mail addresses. It will also include photographs, videos, films and similar material.

"Processing" means anything that is done with, or to, the Personal Data such as using their address to send communications to them and/or others, including him or her in a directory, using photographs in publications, on notice boards for publicity purposes or on websites. It also includes the storing of the information and eventually its destruction.

The "**Data Controller"** is the person, or body, deciding all aspects of how the data is to be used , how it is to be stored, retrieved and destroyed. In the context of St Saviours this will be the PCC. The vicar is a separate legal person as far as the GDPR is concerned and is responsible as the Data Controller for any data that he might hold about individuals.

The **"Data Processor"** is the person who actually does things to the data on the authority of the Data Controller in the course of it being used - such as the listing of addresses for a posting, inclusion of a photograph in a publication or on a notice board or the inclusion of the photograph and other information about a person on a website.

The Data Protection Principles

Data Protection legislation is underpinned by eight "Data Protection Principles" which are in essence a code of good practice for processing personal data. These Principles are laid down in the DPA1998 and are also incorporated into the GDPR. Anyone who processes personal information must comply with these eight principles.

The Data Protection Principles are as follows:

1. The data must be processed lawfully, and in a transparent manner as far as the individual is concerned;
2. The Data must be obtained for specific, relevant and legitimate reasons which must the explained to the individual and any further processing must not be incompatible with those reasons;
3. Data must be relevant, sufficient, and limited to what is necessary for the purpose(s) for which they are used;

4. Data must be accurate and kept up to data with every reasonable step being taken to ensure that inaccurate data is corrected or erased without delay;
5. Data kept in a form in which the subjects are identifiable must be kept for no longer than is necessary for the purposes for which the data was obtained and used;
6. The processing of personal data shall be in accordance with the rights of the individual;
7. Appropriate measures shall be taken to ensure the security of personal data, to protect the data against unauthorised or unlawful processing and to guard against its accidental loss, damage or destruction;
8. Personal data shall not be transferred to other countries unless that country ensures an adequate level of protection for the rights and freedoms of the data subjects regarding the processing of the data, and that data is not transferred to other countries without such adequate protection. (unlikely to be relevant to the PCC!)

Both the DPA1998 and the GDPR make the Data controller – that is the PCC – responsible for complying with these principles regarding all personal data for which they are the Data controller. Failure to do this can lead to a significant fine.

Accountability

The GRDR introduces a new principle – "Accountability" - into the Data Protection area. This principle means that the Data Controller must be able to demonstrate that it has complied with the Data Protection Principles. It will not be enough to simply state that it is compliant. The Data Controller must be able, by producing evidence, to prove that it is complying with the principles. In order to be in a position to do this all of the PCC's documents relating to data protection must be kept in good order and accessible. The documents that will be needed for this purpose are extensive and include the "Data Protection Policy" put in place by the PCC, and records of all subsequent decisions affecting it, such as, for example, any revisions or changes, or any review of its working that may be carried out. It will include records of decisions relating to the nature of the Personal Data that the PCC holds on individuals, and maintain a record of all processing activities for which it is responsible, such as those listed in Appendix 1. Evidence of compliance also includes records of attendance at training events.

There is a responsibility placed on Data Controllers to ensure that appropriate measures are in place, whether on paper or electronically, to hold Personal data securely. In order to ensure the PCC's compliance with the principles underlying data protection it will therefore be necessary to be able to show that this responsibility is being discharged.

The Rights of individuals

As well as placing a greater emphasis on the concept of "accountability" The GDPR also stresses the need for "Transparency" and "Openness" when dealing with Data subjects and in the collection of their personal data . The GDPR gives more unambiguous rights to the individual in respect of how personal data is collected and processed. In particular, it gives the individual greater access to the information held about them and a greater ability to have some control over that data. Importantly, and why these rights must be clearly understood and observed, as well as the contact details for the Data Controller – such as the address of the PCC secretary - the Data Subjects must also be given the contact details for the Information Commissioner's Office (the ICO). This is to allow them to contact these bodies should they believe that their rights have been infringed or violated .

The rights themselves are very similar to those included in the DPA1998 and are:

1. *The right to be informed*; this means that the Data Controller must provide the Data Subject with information such as who they are, the purpose(s) of collecting the data, and how this falls within the "legitimate interests" (see below) of the Controller. Further, this information must be given in a concise and transparent way, and written using clear language that can be easily understood by the subject. This information should also be easy to access by the Data Subject.

2. *The right of access;* the personal data should be easily accessible to the data Subject so he/she can have indications of how it is being used and be able to test the lawfulness of it. If asked for this information it must be given to the Data Subject without charge unless the request is "without foundation, unreasonable or repetitive."

3. *The right to rectification*; where personal data is found to be incomplete or inaccurate the Data Subject has the right to have it rectified. Further, where data has been supplied to third parties then they too must be informed of any rectification. The Individual has the right to be informed of who these third parties are.

4. *The right to erasure*; this is also known as the "right to be forgotten". The reason for this is to allow the Data Subject to ask for the removal of

his/her personal data for various reasons. For example where the original purpose for which it was collected has been achieved and the data is therefore no longer needed and there is no longer a good reason why it should continue to be held. It may because his/her consent has been withdrawn or because the data has been unlawfully processed.

5. *The right to restrict processing*; the Data subject has the right to block or suppress the processing of personal data – perhaps, for example, he/she is contesting its accuracy or lawfulness. In such cases processing must be restricted until the accuracy of the data is verified. However the Data Controller may continue to store the data during a restriction but cannot process it.

6. *The right to data portability*; this is the right for an individual who has given consent for the personal data to be processed and now wants to obtain their personal data and reuse it for another purpose of their own. This right only exists where the processing is carried out by electronic means.

7. *The right to object*; Data Subjects have this right where the purported legal basis of the processing is based on the 'legitimate interests' of the Data Controller (see below), which they do not agree with, or where direct marketing or the processing of data for the purpose of "scientific/historical research and statistics is involved .

8. *The right not to be subject to automated decision-making including Profiling;* this is where a decision affecting the Data Subject is made by automated means and without human intervention. It is very unlikely that this will be relevant to the work of the PCC.

A general point that applies to a number of these rights concerns the process of making the complaint, or calling on the Data Controller (i.e.the PCC) for action. Action must now be taken by the PCC to deal with the matter and respond to the Data Subject ***within 30 days***, unless there are extenuating circumstances to justify a delay. Previously the time for a response/action was 42 days. What this means for the PCC is that it must ensure that it has data storage, access and retrieval systems in place which will allow this deadline to be met.

The need for a 'Lawful Basis' for processing

The current DPA1998 requires Data Controllers to satisfy one of the "conditions for processing", which it lists. The GDPR also requires that in processing data Principle 1 should be satisfied by having a valid 'lawful basis'. This means that

the PCC must establish, and document, the 'lawful basis' that it claims for the processing of data that it is responsible for. If a 'lawful basis' cannot be found that fits its intended processing of personal data then to do anything with it would be in breach of this first principle and not lawful. This would trigger the individual's right to have that data erased.

Secondly, for most of the acceptable 'lawful bases' the processing has to be necessary, and done only for the purpose for which it is intended and which purpose cannot be reasonably achieved in some other less obtrusive way.

Thirdly, after the date when the GDPR comes into effect, the decision the PCC about which of the acceptable 'lawful bases' it is going to adopt must be made before the processing of any personal data . Furthermore, once the PCC has decided which lawful bases it will be claiming for its processing they cannot be changed later to meet another previously unidentified purpose. At least not without a deal of trouble.

Finally, in order to meet the obligations for accountability and transparency, the basis for the lawful processing of data must be clearly documented. The PCC must also tell people upfront about the 'lawful basis' it is using to process their personal data. This is best done by including this information in our "privacy notices" (see below).

The GDPR sets out six 'lawful bases' – similar to the present law - for processing at least one of which must be chosen; there is nothing to stop more than one being chosen. However only two of these 'lawful bases' can be seriously considered by the PCC as applying to the processing it would be doing. The other four, below, do not apply to the PCC's work:–

- It is necessary in connection with a contractual arrangement with the individual;
- It is necessary to comply with a legal obligation;
- It is necessary to protect somebody's vital interests; and,
- It is needed to perform a task in the public interest or to fulfil an official function.

The two which do apply to the PCC's activities, and need to be seriously considered are:-

- That the individual has given their clear and unambiguous consent for the processing of their personal data for a particular specified purpose; and
- The processing is necessary for the PCC's legitimate interests, or those of a third party unless there are good reasons to protect the individual's data which override these legitimate interests.

In choosing our 'lawful basis(es)' the PCC must be able to demonstrate that those 'lawful bases' actually apply to its particular purpose(s).

1. The Individual's Consent

The first of these bases for "lawfulness" is "consent".

In requesting the consent of an individual this must be done in a way that does not confuse it with other terms and conditions; it must stand out, be concise and easy to understand. The request should also provide the individual with details of who the Data Controller is together with a contact address, and also the address of the Information Commissioner (the "ICO") who they can make any complaint to.

One rationale for consent as a basis of "lawfulness" is that it is seen as giving a large measure of control to the individual. It is important then that the individual supplying the consent is made aware of his/her rights; in particular the right to withdraw their consent at any time and to require the use of their data to stop and/or be erased. It should be made easy to withdraw consent.

Before an individual can give consent they must have had the nature and purpose(s) of the processing of the data explained to them - and understands them. They must then be given clear control over their decision. For example it is not acceptable for the consent to be assumed if the individual does not un-tick a box if they do not want to consent. There must be a positive opt-in which must be clear and unambiguous – and recorded in writing - for it to be valid.

A downside of using "consent" alone as the 'lawful purpose' is that it is only valid for the particular purpose(s) for which it is asked. Thus specific consent must be obtained for each particular purpose which it is intended to use consent for. Blanket, all inclusive, consent is not permissible. This means that individuals who may be involved a number of different church functions may have to be asked to give their written consent a number of times which could be seen as irksome.

It may be good practice to obtain consent from an individual to get their buy-in to the PCCs use of, their Personal Data. However, but this does not mean that consent is always appropriate as a 'lawful basis' - and it can be restricting. If the Individual cannot be given real choice and control over how the data is used, it is more appropriate use another of the 'lawful bases' which would allow the processing of data without consent. The most appropriate, and the one giving the widest range for processing, is "Legitimate interest"

2. Legitimate interest

The sixth basis for "lawfulness" is that the processing is in needed for the PCC's 'legitimate interests'. A change that has been made as a result of the GDPR is that, in addition to the PCC's own interests, wider interests can now be taken into account such as those of a third party. However the "legitimate interests" basis for "lawfulness" will only be valid provided that they are not overridden by

the interests of the Data Subject. For example, if the processing would cause the individual unjustified harm then it is likely that their interests would override the PCC's. However provided that there is a clear justification, then the PCC's interests can still prevail in the event of a conflict.

The advantage of "Legitimate interests" as the 'lawful basis' is its flexibility – although it may not be appropriate in all circumstances. It would cover those activities which are necessary for the efficient management of the organisation. For example the use of rotas to ensure the running of various functions – such as the - servers, readers etc, coffee/tea rotas - would fall into this heading. Consent of those whose names and contact details are given on the rota will not therefore be required.

Where it is intended to process Personal Data under the 'legitimate interests' basis the PCC will be responsible for considering and protecting the person's rights and interests. In this respect the first question that should be asked is: - "Would the use of the data for a particular purpose have a minimal privacy impact?" The second question should then be: "would the individual reasonably expect the data to be used in this way?" Further, although consent is not involved, a person may still object to the PCC's use of this basis for lawfulness in processing his/her data and they do have a right have it erased.

Before resorting to the use of this basis for "lawfulness" in the processing of personal data for a particular purpose there are three tests which should be met:

- **Purpose:** What is the legitimate interest in the case of this particular purpose?
- **Necessity:** Is the processing necessary to achieve this purpose? Or can the purpose be achieved in some other less obtrusive way – if so then this basis will not be appropriate.
- **Balancing:** How does the processing balance against the Data Subjects interest, right and freedoms?

A more detailed list of the questions which should be considered will be found in appendix 2.

In order to rely of "legitimate interests" as a basis for processing personal data the PCC must identify, and list what these interests are and assess their appropriateness as above. (Referred to in the GDPR as" Legitimate Interest Assessment (LIA))". They must then be agreed and a record of the outcome of the LIA kept. It should be kept under review and brought up-to-date if there has been any significant changes in the purpose or other aspects of the processing. This will help to demonstrate compliance if called to account in respect of the GDPR's accountability principle. Details of these legitimate interests must also be included in the in our privacy notice. A preliminary list of interests for St Saviours is in Appendix 3.

When not to use 'Legitimate Interests' as the basis for "lawfulness".

If the use of the data will be in ways which are not understood by the Data Subjects, or which are not reasonably expected by them, then this basis for lawfulness should be avoided. The same applies where it is thought likely that some people, if the purpose was clearly explained to them, and understood by them, would object. In this case however the "Consent" route is also likely to be futile. In such cases then either the data cannot be processed, or a compelling reason(s) to over-rule the individual exists or else another basis can be found. In the PCC's case this latter is very unlikely. This aspect should be given careful consideration when drawing up the list of "Legitimate Interests".

Special cases.

The DAP1998 and the GDPR both have provisions for the treatment of "sensitive data" or "special category of personal data" respectively. This is data which, if processed, would reveal information features of the individual - one of which is his or her religious beliefs. Under GDPR processing such information is prohibited unless some other conditions can be met.

As members of a church community, such as St Saviours, it is likely that under the GDPR some, or all, of our members will be regarded as "Special Data Subjects" on the grounds that their data may reveal information about those individual's religious beliefs. Their data would then be regarded as "Special Category Data" and processing will be prohibited unless, in addition to having a 'Lawful basis' as normally required, one of ten exceptions in the GDPR can be invoked to allow processing. The most appropriate one for the PCC would be that St Saviours is a "not–for-profit body with a religious aim". This will allow it to process "Sensitive", or "Special Category Data". However the way this data can be used is restricted to processing relating only to the members and former members of the church and "persons having regular contact in connection with its purposes". The data could therefore be used for parish communications within these groups but cannot be disclosed to anybody outside these groups without the consent of the Individual. This has implications for activities such the use of photographs on billboards or posters, and particularly for a Parish Website. Where consent is being relied on for the processing of this "Special Category Data" the conditions of consent for the use of an individual's data are more stringent than normal. Thus the consent of the individual must be quite explicit and in the individuals writing.

Children

In general Children have the same rights as adults where Data Protection is concerned but GDPR explicitly states that Personal Data of Children "merits specific protection." This is particularly true where a child's Personal data is being used for marketing. Where consent is the "lawful basis" particular

concern will be the level of competence of the child. GDPR has set the age of competence for providing consent to their personal data being processed at 16. For children under this age the processing of their personal data will only be lawful if consent is given by someone with parental responsibility for the child. The PCC will be responsible verifying the name and age of the child, identifying the person(s) with parental responsibility and assuring itself that the appropriate consent has been obtained.

Wherever possible efforts should be made to ensure that the child understands which of their details will be used by the PCC and for what purpose. A child-friendly Privacy Notice should therefore be available. When "legitimate interests" is used as the 'Basis of Lawfulness' the PCC will need to ensure that all the risks and consequences of using the data have been identified, and safeguards appropriate for children put in place.

Children have all the rights an adult has and in particular the rights to object to their Personal Data being used, or to have it removed. This is likely to be particularly relevant if the child, when older, wishes to have his/her data removed after the original consent had been given by the parent. There should therefore be a child-friendly mechanism for this to happen.

It should be noted that if the draft Data Protection Bill becomes law post-brexit the age at which a child may give their consent will be reduced to 13 years

Consent Forms and Privacy Notices

Consent forms

Where Consent is being used as the "Basis for Lawfulness" the law requires a Data Subject's consent to be in writing; it should be unambiguous and clearly separate from any other matters dealt with on the form and it should be made clear that there is an option to refuse consent. In the case of consent to be given for sensitive data (or special category data) the wording on the consent form, and the statement provided on it by the Data Subject, must make it clear that the consent given for a particular process(es) is explicit. In these cases there should not be any opt in/opt out by the un-ticking of a box

Privacy Notices

The first principle of data protection is that personal data must be processed fairly and lawfully, and in both the DPA1998 and the GDPR a key element in the collection and processing of Personal Data is transparency – that is informing the individual about how his/her data is to be used, who is going to use it, and how long it will be retained etc. The DPA1998 requires the individual to be given;

- the name of the data controller;

- the purpose(s) for which the information will be processed; and
- "any further information which is necessary in the specific circumstances to enable the processing to be fair."

To these the GDPR has added the requirement for the information to be;

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

A more complete listing of the information that should be considered for inclusion in the Privacy Notice is given in Appendix 4.

Where the subject of the data is a child then the GDPR requires that the Privacy Notice should be adapted to take account of the level of comprehension of the age groups involved.

To enable the data subject to give consent he/she must know what they are consenting to. Therefore the Privacy Notice must be provided before or with the consent form.

Security

The awareness of the importance of the protection of Personal Data by all concerned with the handling of it is stressed in the GDPR. This is not confined to the way in which Personal Data is acquired and processed, but also to the way in which it is held and stored and also ensuring that the data is not held for any longer than is necessary for the purpose for which it was collected. The GDPR introduces a new requirement with regard to security - "*Data protection by design and by default*". This means putting in place both technical and organisational measures to ensure the safeguarding of the Personal Data. This is particularly important when new policies are being considered which may have privacy implications, when new IT systems are being developed for the storing and accessing Personal Data or when the data is being used for a purpose other than that for which it was acquired.

What happens when there has been a breach security?

The GDPR makes provisions for when a breach in security of 'personal data' occurs as a result of accidental or unlawful action. Where there is a serious risk that a breach will to result in harm to the affected individuals (e.g. identity theft), the PCC, as the data controller, will be responsible for notifying the Information Commissioner's office as soon as possible -

and not later than 72 hours of discovering the breach. The PCC will then have to provide details of the breach, its potential consequences and action to be taken to deal with the situation and mitigate any possible adverse effects. These details of the breach should also be documented in case the ICO needs to check that the PCC has complied with the Regulation. The PCC should also inform those whose data has been affected by the breach.

Next Steps –

What must the PCC do now

- Establish and agree our "Basis of Lawlessness - Before 25th May
- Decide & record the Data policy - Before 25th May
- Create a standard or model Consent form and Privacy notice - Before 25th May
- Review any existing Consents and replace them if they do not conform to the new Law.
- Review storage, retrieval and destruction arrangements and security measures.
- Decide retention times for Personal Data

Conclusion

The information provided above is based upon the existing Data Protection Law (The Data Protection Act 1998) , the EU's General Data Protection Regulation (GDPR) coming into effect on the 25th May 2018 and the Draft Data Protection Bill going through its Parliamentary stages and which will come into effect post-Brexit.

St Saviours along, it must be suspected, with many other Churches has been lax in its compliance with the existing Law. The new law has received considerable (last minute) publicity recently and it is likely that the powers that be will be more rigorous in the monitoring of compliance. The Information Commissioner's Office has powers enabling it to call on any organisation to account under the "accountability" principle. It is important therefore that the PCC and the Incumbent – as a separate legal entity – are familiar with the requirements and their responsibilities under the existing and future Law. In particular we must be ready to observe the requirements of GDPR from its start date.

The new Law gives more power to the Data Subject than hitherto. Their rights must be drawn to their attention in the Privacy Notices and consent forms and so they are now in a better position to ask questions about the use of their personal data, and to call Data Controllers to account. They also have access to the ICO if they need to complain about any infringement of their right.

Members of the PCC are therefore urged to familiarise themselves with the basic tenets of the Law, as outlined above, and ensure that they discharge their responsibilities correctly in the future.

Appendix 1.

Keeping Records of processing activities

The following information must be recorded and maintained by the Data Controller:

a) the name and contact details of the controller;
b) the purposes of the processing;
c) the categories of recipients to whom personal data has been or will be disclosed;

d) a record of all categories of processing

e) a description of the categories of—
    a. data subject, and
    b. personal data;
f) an indication of the legal basis for the processing operations for which the personal data is intended;
g) where possible, the envisaged time limits for erasure of the different categories of personal data;
h) where possible, a general description of the technical and organisational security measures appropriate to processing of the personal data.

Appendix 2.

Identifying legitimate interest(s).

1. **Consider the purpose(s) for which the data is to be used :**

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

2. **Apply the necessity test:**

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

3. **Do a balancing test.** Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

Appendix 3

What are our legitimate purposes?

"Statutory"/regulatory

- Registers
- Electoral Roll
- Gift Aid
- DBS
- Safeguarding

Management

- Financial Records/Accounts
- PCC papers
- Duty Rotas
- Directories *
- FWO and Donors

'Functioning'

- Friends members*
- Communication*
- Information*
- Fundraising*
- Event helpers (i.e. XTF)*
- Publicity material*
- Website*

*Items where consent should be obtained

Appendix 4

Information to be provided in Privacy Notices

- Identity and contact details of the Data Controller and where applicable, the Controller's representative and the data protection officer
- The purpose of the processing and the legal basis for the processing
- The legitimate interests of the Data Controller or third party, where applicable
- The categories of personal data
- Any recipient, or categories of recipients, of the personal data
- The retention period or criteria used to determine the retention period
- The existence of each of Data Subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority (i.e the ICO)
- The source the personal data originates from and whether it came from publicly accessible sources

-Not relevant to St Saviour's situation

- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data
- The existence of automated decision making, including profiling, and information about how decisions are made, the significance and the consequences.