****

**GDPR Briefing Document for Liberal Judaism Communities**

There has been a lot of media interest about the implementation of GDPR, and we are aware of the concern regarding the impact that this will have on Liberal Judaism communities and the records that you hold. Whilst we do not want to underestimate the impact of the legislation on communities, particularly on processes around record-keeping and sharing information, we have been reassured by a number of reports that the initial work that needs to be completed is straightforward, and this briefing aims to set out the basics that need to be in place as soon as is practicably possible.

Attached to this document you will find a presentation from GDPR expert Tim Turner, who delivered GDPR training for Liberal Judaism and Reform Judaism. His final page highlights actions to be taken now; whilst the Information Commissioners Office (ICO) will not expect everyone to be fully compliant by May 25th, there will be an expectation that **up to date privacy notices will be in place, along with a complaints procedure and plan for the other changes needed**. A good first step is to ensure that there is at least **a data protection lead appointed**, so that it is clear who is in charge of the project and to whom complaints and issues should be addressed.

A straightforward checklist of the most critical actions can also be found at: [www.parishresources.org.uk/wp-content/uploads/GDPRchecklist.pdf](http://www.parishresources.org.uk/wp-content/uploads/GDPRchecklist.pdf)

As well as this briefing we can highly recommend the ICO small business helpline if you need help on a specific issue. When we have used it we have found the assistance to be clear and practical – they can be called during working hours on **0303 123 1113 (select option 4) We are also happy to help in any way that we can, please do not hesitate to call Shelley on 020 7631 9835 or email** shelley@liberaljudaism.org **and we will do our best to assist. Finally, we hope that as communities work towards GDPR compliance, we can share good practice and examples of policies, procedures and statements via the Resource Bank. If you have something to share, please do not hesitate to be in touch.**

**Layout and Purpose of this briefing document**

The purpose of the document is to cover the basic issues and provide links to further information and templates, as well as Liberal Judaism policy where this exists. The amount of information available about GDPR is enormous but the ICO website is a good place to start; we’ve picked relevant pages where possible. Liberal Judaism has used templates available via Certikit as a way of moving the process forward quickly; these may be changed as guidance and other sources of information become available. This document is not intended to be exhaustive and will be expanded and edited as some areas of work are completed. This is still a work in progress, clarification and final guidance from the ICO is still due in some areas.

There is a simple glossary at the end of this document.

**Background**

GDPR stands for the General Data Protection Regulation (GDPR), which comes into force in the UK on May 25th 2018. GDPR is intended to improve the protections available to individuals in relation to their data, and builds on the current Data Protection Act enshrining the following rights for individuals:

1. The right to be informed – this is mainly covered in practice by privacy notices.
2. The right of access – individuals have to be given the right to access their data, to check the accuracy and lawfulness of what is being held. This is covered in practice by subject access requests and subsequent action.
3. The right to rectification – the individual has the right to have their data rectified if is incorrect and for it to be rectified if it has been held by any third parties.
4. The right to erasure – the individual has the right to have their information removed if there is no compelling reason for processing and if they have previously given consent. There are legal obligations to hold data – for example for safeguarding purposes – which override this right.
5. The right to restrict processing – the individual can stop you using their data under some circumstances.
6. The right to data portability – obtain and use data for own purposes. Will vary.
7. The right to object – the individual has the right to refuse processing in some circumstances – this is less likely to be an issue if consent is the basis for processing.
8. Rights in relation to automated decision making and profiling – this is not likely to be an issue for Liberal Judaism or communities.

Pages 4-6 of the Parish Resources guide to GDPR offers a lot more detail on this:

<http://www.parishresources.org.uk/wp-content/uploads/Parish-Guide-to-GDPR.pdf>

Whilst this seems intimidating at first, it is a good opportunity to take a look at relationships and how information held by the community is stewarded; it is a good opportunity to check in with best practice and improve transparency and accountability to members.

This document will use the ICO document “Preparing for the General Data Protection Regulation (GDPR): 12 Steps to take now” to break the work needed for GDPR into steps. It can be read here: (<https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf> )

**1. Awareness**

**Key issue**

Any staff or volunteers need to be aware of the GDPR and how it affects data processing and collection in their specific area of work. It needs to be understood by the Council/Trustees of the community and data protection principles need to be incorporated into project planning and review, risk assessment and operational work.

**What Liberal Judaism has done so far**

Within Liberal Judaism, we have ensured that key staff have received detailed training and all staff will receive training on GDPR before implementation. We will repeat data awareness training annually for the whole team as part of keeping our systems under review, and new staff will receive data awareness training as part of induction. This training will be delivered by the Data Protection Officer. Induction training will be delivered through the Educare Data Protection module for all staff.

**Resources**

Liberal Judaism subscribes to Educare, which has a module on Data Protection. Please contact us if you would like access and we will create a free account for you.

The ICO has a series of resources – including toolkits and videos, on their website:

<https://ico.org.uk/for-organisations/resources-and-support/>

**2. Audit**

**Key Issues**

In order to ensure that the provisions of the GDPR are being met, it is critical to understand what data is held by the community and where. This process might bring up a few surprises! An action plan can be built once any issues are known.

According to ICO advice, keeping a full record of personal data meets the GDPR principle of accountability; a key issue throughout is the need to document and potentially show evidence of policies, procedures that are in place.

The audit will also bring up where data is stored, but also think about whether it is ever downloaded – for example synagogue membership databases. If is kept in the cloud, are there rules in place about downloading data, or what is done with it once it has been used? What level of encryption is used for data stored on laptops, or computers at home? Who has access to shared drives – when someone leaves a role, is their access to Dropbox/google drive/similar restricted, are passwords changed? A key principle to protect data and prevent breaches is to limit the number of people who have access to it to, ensuring it is only shared where necessary. Creating email addresses for specific community roles might also be worth considering, so that there is less potential overlap between personal accounts and those linked to community roles.

An action point that might arise from the auditing work is the creation of a data management policy which sets clear guidelines for how data is accessed and how that access is managed. We will share the Liberal Judaism (ULPS) policy once it is complete.

**What Liberal Judaism has done so far**

A personal data mapping procedure has been adopted and is attached. Each area of personal data has a separate personal data questionnaire which feeds into a personal data inventory; a sample of a personal data questionnaire is attached. Action points from the inventory feed into a ‘to do’ list, with allocated actions, dates etc.

Finally, as result of mapping the data we hold, we have deleted a lot of out of date material that no longer needed to be held. This was electronic and paper based and included old email accounts.

**Further Resources**

There are a number of templates available for data audits:

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

The attached document lists ‘Dos and don’ts’ of data protection and is a good starting point for consideration of how to store data safely.

**3. Privacy and Consent**

**Key Issues**

**Privacy and Privacy Notice**

The emphasis within GDPR on transparency and accountability adds value to the sort of information that has to be given when collecting personal data, and to include as a minimum information about the right to complain, data retention periods and the legal basis for data processing. This has to be done in a way that is concise, clear and easy to understand, and free of jargon.

Some of the most significant changes relate to privacy notices, which now must give information about:

* What information is being collected and who by
* What this will be used for
* The lawful basis for processing
* How it will be processed and stored
* How it is shared (if at all)
* How long data is kept for
* Individual rights and personal data
* How to complain and who to contact in the community – and further sources of help.

It is essential to review your privacy notice, especially the section that outlines the lawful basis for processing and to make this publically available. It is also a good time to review your website privacy policy.

Liberal Judaism also recommends sending your privacy notice with any forms (or putting this as a link online where forms are online) whenever it is amended, as explicit consent can only really be meaningfully sought if someone understands what they are consenting to and what you will do with their data.

For more information about what should be in a privacy notice, visit the very comprehensive section at the ICO website:

<https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control>

**Lawful Basis for Processing**

This is where it is essential to highlight your reasons for processing personal data, essentially to make the case for why you need to hold it at all. This is an interesting way to check and clarify why you are holding data, and what is essential (and what really isn’t) Whilst there has been a lot of focus on consent, **all of the bases for processing are equal,** and apply to different types of information and relationships. The basis you chose has to be included in your privacy notice/s and there can be implications if you chose to change it at a later date – so it is worth spending time to get this right. (When we have been unsure in this area, we have found the ICO small business helpline to be an excellent resource)

The first step is to ensure that your data audit includes all potential areas of data that you hold, and then to explore these on a case by case basis.

Article 6 of the GDPR sets out the various legal bases for processing personal data. In the community context the most relevant include:

• Legal obligation, (e.g. a legislative requirement, such as processing gift aid applications);

• Legitimate interest, (e.g. administration of community leadership contacts);

• Consent, (e.g. sending out a newsletter);

• Contract (e.g. agreements for hiring out a hall, agreement to provide burial as part of a scheme);

Some of the personal data processed will be classed as sensitive (included in the “special categories of personal data” under the GDPR) because it reveals “religious belief” and additional requirements are in place if you process this kind of data. You will need to identify both an initial basis for processing (Article 6) and an additional basis (as listed in Article 9). In a community context these additional bases are most likely to be:

• Explicit consent from a person; or

• Legitimate activity - where the processing relates to either members or former members or to individuals with whom there is regular contact but is not disclosed to any third parties outside the community without consent.

(Adapted from <http://www.parishresources.org.uk/wp-content/uploads/GDPR-Parish-Guide.pdf> )

Please note that if legitimate interest is to be used a basis for processing, it is necessary to conduct a legitimate interest assessment, which tests necessity of the processing and the balance of benefits and potential issues for the data processor and the data subject. This provides clarity and transparency about why you are processing this data and is a useful process to engage with.

The Data Protection Network has produced an excellent guide to legitimate interest, which is only available after signing up to their website. It can be found here:

<https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/>

**Consent**

**How should you obtain, record and manage consent?**

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. Include:

* the name of your organisation;
* the name of any third party controllers who will rely on the consent;
* why you want the data;
* what you will do with it; and
* that individuals can withdraw consent at any time.

You must ask people to actively opt in. Don’t use pre-ticked boxes, opt-out boxes or other default settings. Wherever possible, give separate (‘granular’) options to consent to different purposes and different types of processing.

Keep records to evidence consent – who consented, when, how, and what they were told.

Make it easy for people to withdraw consent at any time they choose.

(From <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/> )

Consent can be requested for a number of issues simultaneously; it is not necessary to request it on several forms. The ICO website has an excellent section on consent:

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

There are special provisions for seeking consent from children; for anyone under 13 a parent or guardians specific consent is required to process their data. This should be made explicit on any forms, and is of particular concern if data is shared with LJY-Netzer/Liberal Judaism. This also means that consent notices have to written in a clear manner that young people can understand. LJY-Netzer will offer sessions to their members on privacy and information at Kadimah this summer – if you need to gain consent from young people this is an excellent opportunity to engage with younger members in a meaningful way.

**What Liberal Judaism has done so far**

* Clarified the areas under which we have a lawful basis for processing.
* Rewritten our privacy policy for some processing activities – more are to follow (an example is attached)
* Changed our consent forms to improve wording and clarity. (A sample consent form is attached)
* Created notices to confirm that we are processing data using legitimate interest as a lawful basis, and seeking information about preferences (an example is attached)

We are waiting for specific advice about privacy notices and consent with regard to recruitment and employment. We will share our processes as soon as we have them.

**Further Resources**

There is useful information on this page, including the link to a draft privacy policy:

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

**4. Subject Access Requests**

**Key Issues**

Subject access requests are an important right, as they enable individuals to check that the data held on them is correct and up to date and to challenge if this is not the case.

Subject access requests are not a new right but GDPR has reduced the time period for dealing with them to one month, and in most circumstances a fee cannot be charged.

The ICO summary of subject access requests can be found here:

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

**What Liberal Judaism has done so far**

* We have written a subject access request policy and form (attached)
* Considered data portability within the systems we currently have and identified what we can offer.
* Clarified processes for deletion and what can be deleted.

**5. Data Breaches**

**Key Issues**

A policy needs to be in place to detect, report and investigate personal data breaches. The term breach covers a wide range of scenarios, including:

…a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data

* Personal data breaches can include:
* access by an unauthorised third party;
* deliberate or accidental action (or inaction) by a controller or processor;
* sending personal data to an incorrect recipient;
* computing devices containing personal data being lost or stolen;
* alteration of personal data without permission; and
* loss of availability of personal data.

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

All data breaches must be recorded and data breaches that pose a risk to an individual must be reported to the ICO within 72 hours of becoming aware of the breach. Individuals may also need to be notified of the breach, as soon as possible if there is the risk of loss or distress. This does not have to be a financial loss, for example, it can be any loss of data that might cause embarrassment or personal distress.

A process for identifying and investigating breaches is also required.

**What has Liberal Judaism done so far?**

* Written a data breach notification form and procedure (attached)
* Considered how a breach could take place as part of risk audit and started to create a data management policy for LJ staff that aims to minimise the risk of a breach

We are still working on clarifying roles and responsibilities.

**Further Resources**

The ICO defines a breach and offers a useful checklist on this page:

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

**Next steps**

In addition to the areas of work identified above, we will be:

* We will be sharing the work we are doing to comply, including our data management policy.
* We will encourage communities to share any policies or procedures that might be of use, especially when looking at issues specific to running a Jewish community.
* We will be working on privacy impact assessments and privacy by design.

**Glossary of Terms**

**Consent**- freely given, specific, informed and explicit consent by statement or action from an individual signifying agreement to the processing of their personal data

**Data Controller** - the entity that determines the purposes, conditions and means of the processing of personal data (for example Liberal Judaism, your community)

**Data Erasure** - also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

**Data Portability** - the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller

**Data Processor** - the entity that processes data on behalf of the Data Controller (for example a payroll service)

**Data Protection Authority** - national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

**Data Protection Officer** - an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR. Not all organisations require a data controller.

**Data Subject** – an individual whose personal data is processed by a controller or processor

**Derogation** - an exemption from a law

**Encrypted Data** - personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

**Enterprise** - any entity engaged in economic activity, regardless of legal form, including persons, partnerships, associations, etc.

**Filing System** - any specific set of personal data that is accessible according to specific criteria, or able to be queried

**Personal Data** - any information related to an individual or ‘Data Subject’, that can be used to directly or indirectly identify the person

**Personal Data Breach** - a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

**Privacy by Design** - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition

**Privacy Impact Assessment** - a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

**Processing** - any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

**Profiling** - any automated processing of personal data intended to evaluate, analyse, or predict data subject behavior

**Pseudonymisation** - the processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as said additional data stays separate to ensure non-attribution

**Recipient** - entity to which the personal data are disclosed

**Right to be Forgotten** - also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data

**Right to Access** - also known as Subject Access Right, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

**Subject Access Right** - also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

Adapted from: https://www.eugdpr.org/glossary-of-terms.html