Changes to Data Protection:
Guidance for
Triratna Buddhist Centres in Europe

Contents:

Introduction:

The **General Data Protection Regulation (GDPR)** is due to take effect May 25th 2018 at which point organisations have to be compliant (after what will have been a 2 -year transitional period). It will replace the current '**D**ata **P**rotection **A**ct' which has been in place since 1998 (when only 10% of households had internet connection and facebook and google didn't exist …)

The GDPR aims primarily to
1) give control to individuals over their personal data (e.g. over one's facebook and google data) and
2) unifying the regulation within the EU. DPA was only applicable to organisations established in the UK – GDPR covers any organisation established in the EU or processes personal data of EU data subjects. Brexit will not affect application of these regulations as they will be taken on as a virtually identical set under the name of The Data Protection Bill (DPB).

The regulation applies to any situation where the **data controller*** or **processor*** or the **data subject*** is based in the EU **AND** to organizations based outside the European Union if they collect or process personal data of EU residents (e.g. tbco). Both **personal data*** and **sensitive personal data*** are covered by the GDPR. (for * explanation of terminology see appendix 1)

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA): If your Centre or project is already complying with the current UK data protection law, its highly likely you will be meeting many of the GDPR principles. Do note there is **no charity exemption** to data protection or marketing law.

Most Triratna Buddhist Centres do not need to register (in the UK - with the ICO/ Information Commissioner's Office). This is because we are basically 'membership organisations', run for the benefit of our members and:
"Your organisation was established for not-for-profit making purposes and does not make a profit OR your organisation makes a profit for its own purposes, as long as the profit is not used to enrich others. You must:

- *only process information necessary to establish or maintain membership or support;*
- *only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;*
- *only share the information with people and organisations necessary to carry out the organisation's activities. Important - if individuals give you permission to share their information, this is OK (you can still answer 'yes'); and*
- *only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration."*

If you use CCTV at y our Buddhist Centre you must register with the ICO. The cost for this is currently £35 annually but may be £55 – see appendix.

Fundraising charities like the futuredharmafund, the India Dhamma Trust, and Karuna are in a different position and will probably need to register with the ICO if they also store details of people outside Triratna, members of the general public: You can do the 'Self-Assessment Tool Kit' to check whether you need to register: https://ico.org.uk/for-organisations/register/self-assessment/
Also see page 9

Data Protection Act – the current law

We still need to comply with these **8 DPA guidelines:**

1. **Personal data shall be processed fairly and lawfully:**
    - The data subject must have given their **consent** to the processing.
    - The subject must remain fully informed of how and **why** you are using the data, if not explicitly mentioned at point of collection.
    - You must have a **legitimate reason** for processing the data and you must only use the data for the legitimate reason identified.

2. **Personal data shall be obtained only for one or more specified and lawful purposes.**
    - You must use information only for the specific purpose for which you have permission.
    - You must be explicit to the individual, from the outset, about why you are obtaining their personal data and what you are going to do with it.

3. **Personal data shall be adequate, relevant and not excessive.**
    - You must only hold as much personal data as you need for the purpose - no more. This information has to be relevant and sufficient enough to be able to complete the intended purpose.
      For example, if you want to send out a monthly newsletter you will require solely the names and contact details of its members. You don't need information on age, ethnic background, family etc. as it is irrelevant to the purpose.

4. **Personal data shall be accurate and, where necessary, kept up to date.**
    - While the data is being used for the agreed purpose, it must be monitored for accuracy and kept up to date

5. **Personal data processed for any purpose or purposes shall not be kept for any longer than is necessary for that purpose or those purposes.**
    - If you have created a mailing group for people interested in an introductory course then you are not allowed to then keep it for sending out your monthly sangha newsletter – you'd need to get a new consent. Otherwise after the original purpose is completed, the data must be securely deleted or destroyed.
    - Information may not be obtained and held onto on the basis that it may be useful 'in the future' for as-yet unidentified purposes
    - You need a process in place that makes clear why you are using the data, where it is clear you have thought about how long you will need to keep it for and that you review the process regularly.

6. **Personal data must be processed in accordance with the rights of the individual.**
    - Individuals have a range of rights to know what personal information is processed about them, to put it right if it is wrong, or to stop it being used altogether.
    - This right to obtain a copy of personal data is known as the 'right to subject access'. This states that if an individual requests access to the data in writing, they must be:
        - Told whether, and for what purpose, their personal data is being processed, where the information came from and to whom it may be disclosed.

- Given a description of the data involved and all the information forming their personal data, usually as a permanent copy.
- Told about the logic involved in any automated decision made about them based on the data processed

7. Personal data must be kept secure in order to prevent loss or unauthorised disclosure.

- This includes security of both computer and manual records (such as paper booking forms), including secure servers, back-up and arrangements for confidential shredding.
- This also refers to having security measures to prevent unauthorised disclosure - for example, only allowing certain people access to data and using computer security programs.

8. Personal data shall not be transferred to a country or territory outside the EEA

- Countries within the European Economic Area (EEA) are considered to have adequate legal protection in place to deal with personal data. You may transfer personal data to countries within the EEA on the same basis as you may transfer it within the UK.
- However, you may only send personal data to a country or territory outside the EEA if that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to processing personal data.
- You can find details of countries' adequacy levels on the EU website: ec.europa.eu/justice/data-protection

What is changing with the GDPR from May 2018?

All the 8 DPA guidelines still need to be complied with; **in addition,** there are certain additional requirements: all apply to data already on any mailing list as well as new data.

1. One of biggest changes is **the requirement to obtain *explicit* consent** from data subjects:

- The data subject must consent by **clear affirmative action:** e.g. consent by *ticking,* not *un*-ticking a box
  It is now not lawful to rely on inaction, opt-out, pre-checked fields or silence. There should be no 'pressure' – there must be a genuine choice. The consent must not be buried in other terms & conditions – it should be clear
- The data subject must be provided with a **clear explanation** of the data processing to which they are consenting. The consent wording must explain clearly and intelligibly and precisely the scope and purpose of data processing and the context
- **Organisations must be able to demonstrate that consent was obtained** [for example, have a written policy that is given to all reception volunteers or has been sent out to class leaders; minutes of trustees meeting where this has been agreed;]

The information you need to tell the person is:

1. The data controller's identity and location: i.e. access to name of charity, who the trustees are and the address data is held
2. The purpose of collecting and using their data
3. If you are going to give the data to anybody else (third party). However, in the eye of the law, 'Triratna' is seen as a single body, so e.g. the College of Public Preceptors, is not seen as a 'third party'.
4. That they have rights to access their data and rights to correct it
5. They also have rights to have their data erased ('right to be forgotten') – but if they want to stay a mitra, they need to stay a 'member'.
6. They have the right to withdraw consent and you need to make it clear how they can do it – there should be an easy process in place
7. You need to tell them how they can exercise their rights – who to contact and where and how; have a clear policy that is easily accessible

You can obtain consent
Online: ticking a box, choosing settings, downloading instructions
Offline: signing a data protection authorisation, verbally agreeing, completing a form

Unacceptable method: silence; pre-ticked box, failure to opt-out, **relying on unsubscribe options** or any other passive reaction: so, you can't now just add people to your mailchimp newsletter and rely on the fact that they will just unsubscribe if they don't want to get it!

Consent may include permission to transfer data **outside of the European Economic Area** and such consent makes this lawful: you must be clear in the wording of your consent if cloud services or back-ups are based in the US – or indeed if their data is stored in the US

As before: you are only allowed to use data for the purpose it was given: data collected for one purpose may not then be used for another.

For example, if you obtained their data to send them handouts as part of an introductory course you are not then allowed to keep the data for sending regular newsletters, unless the data subject has given specific consent and you have communicated exactly what you intent to do with it.

2. Another key change is the **increased rights of data subjects;** such as

a) People have a right to ask and be told:

- How and where their data is being processed
- Why their data is held
- What categories of data are being held
- If the data is shared with anyone
- How long this data will be stored and what the criteria are for determining this
- What their rights are in terms of erasure, and to make objections
- The source of their data
- Where they can complain
- They can ask for a copy of the individuals personal data
- If a data subject asks for these rights the controller must pass these requests on to any third parties they have given the data too

b) subject access: you must supply requested data within one month – so you need a process in place how this is going to happen (and you are allowed to charge £10 for this).
c) the right to be forgotten and the right to have data erased
d) there must be an easy process for unsubscribing
e) privacy policies should be easy to read and understand

3. Accountability: the data controller – i.e. in our case the trustees of a Buddhist Centre - are responsible for compliance with the data protection principles and burden of proof now rests more clearly on *them* to show the steps taken to ensure compliance.

- This involves data **security** both in terms electronic and physical records;
- Appropriate **training** for team members and volunteers in data protection
- having data protection **policies** and relevant documents on how data is processed

Checklist for Triratna BUDDHIST CENTRES (& Triratna Groups and most projects)

1) Identify a member of team/ trustee(s) who takes on looking at how your Centre processes personal data.

2) Have an audit of your data storage and processing – you need to find the answers to these kinds of questions:

- Where & how is personal data stored?

- **Consent:** How does your Centre gain consent?
  - Do you give clear information to people at your Centre so they know what their data is used for and what their rights are in relation to it;
  - Do you only use the data you have for the purposes for which consent was given?
  - How can people withdraw consent?

- **Data processing:**
  - Is there a member of your Centre Team who is aware of data protection and regularly looks at the Centre data/ updates or deletes it?
  - Make sure your Centre only keeps personal data as long as necessary and has a process for deleting personal information once it is no longer required.
  - Is there regular **training** in data awareness – in particular, are new team members and volunteers trained up. Do you update this every now and then?

- **Data security**:
  - How secure is your data?
  - How do you destroy data: e.g. shredding paper copies; is all old e-data securely deleted
  - If you have people personal details on any mobile device like a lap top or a memory stick are these always encrypted?
  - Have you looked the degree to which the office is physically secure; are filing cabinets locked?
  - Is the data base held on the office computer accessible by volunteers?
  - Are computer screens inadvertently visible to the public?
  - Does it happen you have private telephone conversations where the public may hear?
  - Is your internet security up to date?
  - Does the Centre use strong passwords as a matter of routine i.e. with an upper, lower case letter, a number and a symbol?
  - How is your data backed up?
  - Have you thought how you can prevent breaches: Is your security software up to date? What will you do if your Centre does accidentally misuse data – have you got a process in place/ a policy that describes what to do.

- **Accountability:** trustees are ultimately responsibility that how the Centre deals with personal data is carried out lawfully.
  - Has data protection been an agenda item so show trustees are informed of GDPR

- Minutes of trustee meetings minutes should reflect that you have considered data protection and acted on your findings:

    - ✓ For example, you have documented that you have taken steps to find out what personal data you hold at the Centre, where that data came from and who it is shared with - i.e. you have had an information audit.
    - ✓ You have identified areas that could cause compliance problems under the GDPR and have recorded these; for example, you have identified that you need to make clearer how you seek, record and manage consent; or that you have reviewed your current privacy notices and have a plan in place to make changes in time for May 2018;
    - ✓ You might refer to the existence of policies and procedures relating to data protection; for example, you have plans in place for how you will handle requests from individuals for access to their personal data within the new timescales outlined in the GDPR (1 month);
    - ✓ The trustees' minutes show that you have asked for a review of the effectiveness of data handling and security controls
    - ✓ You can show you have some form of 'data protection training programme' for team & volunteers at your Centre;
    - ✓ If you offer services/classes directly to children (LBC – after school club), you communicate privacy information in a clear plain way that a child will understand. You have systems in place to verify individuals' ages and to obtain parental or guardian consent where required.

3) Prepare appropriate policies and procedures

- Info for centre team and reception how you ensure that all data you hold is obtained through affirmative consent
- Have processes in place, such as to include "*Find out what information we hold on you*" and "*Remove all information about me*" sections in your privacy policy to give people clear information *****
- On your website, and when taking people's contact details, you need to explain clearly **why** you are collecting personal data and how you intend to use it; **who** you will share it with if at all, and that you are committed to protecting their privacy *****
- People can make **subject access requests** at any time to check the data you hold and what you do with it: have a clear procedure how this can be done
- Training: have an info sheet that you can give to new volunteers who help out at the Centre

**** see separate document entitled 'privacy policy template'***

Further Information:

Read the **ICO's 12-step guide** - available here
In Ireland, the regulator has also setup a separate website explaining what should change within companies.
As well as this guidance, the ICO says it is creating a phone service to help small businesses prepare for GDPR. The service will provide answers about how small companies can implement GDPR procedures and starts at the beginning of November 2017.
And by the end of the year, the ICO will publish a full Guide to the GDPR.
– The full regulation. It's 88 pages long and has 99 articles.
– The ICO's guide to GDPR is long but clear and comprehensive
– EU GDPR is the Union's official website for the regulation. It details all you need to know and has a handy countdown clock for when GDPR will come into force.
– The EU's Article 29 data protection group is publishing guidelines on data breach notifications, transparency, and subject access requests
- guidance from the Fundraising Regulator

Triratna fundraising charities:

It seems very likely that fundraising charities like futuredharmafund, the India Dhamma Trust, and Karuna will need to register with the ICO: You can do the 'Self-Assessment Tool Kit' to check whether you need to register: https://ico.org.uk/for-organisations/register/self-assessment/ - I expect that fundraising charities cannot say 'Yes' to the following:

"Your organisation was established for not-for-profit making purposes and does not make a profit OR your organisation makes a profit for its own purposes, as long as the profit is not used to enrich others. You must:

- *only process information necessary to establish or maintain membership or support;*
- *only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;*
- *only share the information with people and organisations necessary to carry out the organisation's activities. Important - if individuals give you permission to share their information, this is OK (you can still answer 'yes'); and*
- *only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration."*

Much of fundraising involves collecting and storing data:

- contact donors and supporters,
- identify and approach potential new supporters.
- how you do campaigning & marketing,
- managing your volunteers
- recording information about donors and potential donors

And it is clearly not just about maintaining a membership list as most Centres do.

I understand that, basically, fundraising charities need to follow the same guidance as other charities and organisations, and it is to some extent a common-sense approach, putting themselves in the others shoes and considering how you would want your own data to be treated.

Perhaps more than other charities you must take note of the GDPR that says about **explicitly** asking for consent; and that the **purpose** for which you are obtaining and storing data must be "*specified, explicit and legitimate*":

That means must **set out your purposes clearly and unambiguously**, and you can't just say 'fundraising purposes', when that could cover a variety of data uses.

So, one must engage with the discipline of clearly **identifying the charity's purposes** at the outset and you must break down 'fundraising purposes' into its constituent parts. If you want to use data for a second purpose, you will need a persuasive case that what you're doing is not in conflict with the original purpose. If it can be said to be incompatible with the original purpose you cannot use the data

The Fundraising Regulator's guidance recommends these 3 steps:

1. PURPOSE: Establish each purpose (activity) for processing personal data

• Is it Direct Marketing/Fundraising?

• Is each activity similar or different?

• Which channels do you use?

2. LAWFULNESS: Agree the lawful basis for processing for each activity

• i.e. for Direct Marketing to a specific segment, are you relying on opt-in consent, legitimate interest, or something else?

• How long will consent last?

3. FAIRNESS AND TRANSPARENCY

• Clearly publish Privacy Notices at all data collection points, explaining your activities and decisions, along with the rights of individuals to access their data or stop direct marketing.

• Keep copies of privacy notices and an audit trail of approval and their use

Legitimate interest:

GDPR makes it harder for organisations to use 'legitimate interest' as a legal basis for contacting subjects. The controller must now explicitly inform data subjects at the time of collection the purposes of the processing and the legitimate interest it is relying on to process the data. The Fundraising Regulator sets an expectation that **consent should be the legal basis for Charity Direct Marketing (i.e. fundraising)** going forward.

A charity's legitimate interest in furthering their cause must not override the rights of the individual, so the reasonable expectations of the individual based on their relationship with the charity must be taken into account. Ultimately, GDPR is very clear that an individual's choice to say "no" is paramount.

Appendix 1:

Terminology:
Data controller: the organization or the person that collects data from EU residents and that decides the purpose and manner that personal data is used/ will be used: in our case the chair would be the most likely office holder.
Data Processor: the organization that processes data on behalf of data controller – the Centre office team or worker. Processing is obtaining, recording, adapting or holding personal data.

Data subject: the person whose data is collected/stored
Personal data: any information that can be used to identify a person. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address.
Sensitive personal data: includes genetic data, **information about religious and political views, sexual orientation**, and more.

Appendix 2: likely tiers used for assessing fees

Tier 1: Small and medium firms that do not process large volumes of data	Staff headcount below 250; and Turnover below £50M pa; and Number of records processed under 10,000 *Public Authorities should categorise themselves according to staff headcount and number of records only.
Tier 2: Small and medium firms that process large volumes of data	Staff headcount below 250; and Turnover below £50M pa; and Number of records processed above 10,000 *Public Authorities should categorise themselves according to staff headcount and number of records only.
Tier 3: Large businesses	Staff headcount above 250; and Turnover above £50M pa *Public Authorities should categorise themselves according to staff headcount and number of records only.
Direct marketing top up	Organisations that carry out electronic marketing activities as part of their business.

The proposed amounts are:

Tier 1: annual fee of **up to** £55
Tier 2: annual fee of **up to** £80
Tier 3: annual fee of **up to** £1000
Direct marketing top up fee of £20