GDPR update
November 2017

GDPR – as almost everyone knows by now – is the European Union's new General Data Protection Regulation, and it comes into force on **25th May 2018**.

This paper does not give a full account of GDPR. It focuses on what will change from our present legislation, and what charities should be doing to prepare.

There is more on the background and legal process at the end of this paper.

What does GDPR say?

GDPR is an evolution of our current Data Protection legislation, not a radical change of direction. This means that if you are already complying with the UK's Data Protection Act 1998 (DPA) you will be well placed to comply with GDPR.

The basic framework is the same, although there are some differences of terminology. We are still talking about Data Subjects, Data Controllers and Data Processors, although GDPR also refers to Data Subjects as 'natural persons', and to 'Controllers' and 'Processors' without the 'Data'.

We still have Data Protection Principles, almost unchanged, except that the current Principles 6 (Data Subject rights) and 8 (transfers abroad) are taken out of the Principles and dealt with elsewhere.

It is still true that all processing has to meet at least one of a set of six Conditions, but these are now called the 'legal bases' for processing. These are, again, substantially unchanged in GDPR, and include (briefly):

- Consent of the Data Subject
- In connection with a contract
- In order to comply with the law
- In an individual's 'vital interests'
- In the public interest
- In your 'legitimate interests'

"Sensitive personal data" is called 'special categories' of personal data in GDPR. The list is much the same but criminal records and court proceedings are not included, because there is a separate piece of EU legislation about that area. It is still wise, in most cases, to have 'explicit consent' for processing these special categories of data.

As well as complying with the Principles and having a legal basis for processing we still have to be transparent. However, the list of topics about which we may have to inform the Data Subject is much more extensive (see below).

So that's what stays pretty much the same. The **important changes** that are likely to affect charities and voluntary organisations. come under the following headings:

- Changes in the definition of consent
- Using 'legitimate interests' as a basis for processing
- Transparency: what you have to tell people about your processing
- Data Subject rights
- Processing data on children
- Your record keeping
- Data Protection by design and by default
- Your relations with other organisations
- Changes in your relationship with a Data Processor

- Security
- Breach notification
- Data Protection Impact Assessments
- Will you need a Data Protection Officer?
- Transfers abroad
- Fines and enforcement

What you need to do in order to comply will, of course, depend on what your organisation does and how you do it. Some suggested actions are included below, but they may not all apply to you.

Section 1: The GDPR regime

This section describes the main areas where GDPR means that your organisation may have behave differently in future.

Consent

One of the big talking points around GDPR has been the **tightening up the definition of consent**. This now reads:

> *any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or a clear affirmative action, signifies agreement …*

The word 'unambiguous' is new. This means that it is now very difficult – if not impossible – to obtain consent by giving people an opt out box and assuming that they consent if they don't tick it.

Action:
Determine whether any of your current processing is based on assumed consent and stop, unless you can get consent or have another legal basis for the processing.

GDPR also says that in any statement the request for consent must be '*presented in a manner which is clearly distinguishable from other matters … using clear and plain language*'. So, no tricking people into giving consent when they may not realise they are doing so, and no bundling up a number of things into one consent: it now has to be 'granular'.

Action:
Review all the statements where you ask people for consent to ensure that they are clear and unambiguous.

There is another sting in the 'consent' tail. If you are basing your processing on consent you must be able to 'demonstrate' that you do have consent. There is no real guidance yet on what this means, but as a minimum one might suppose that you would need to keep a record of when and how (e.g. by ticking a box) people consented and what they consented to (ideally by reference to the full statement on the data capture form, for example).

Action:
Make sure that your CRM and other record-keeping systems have the capacity to record enough details of consent given – or subsequently withdrawn.

Legitimate interests

The changes to the definition may mean that it will not be possible to use 'consent' in future where it might have been your legal basis for processing in the past.

In many cases your legal basis for processing will be obvious, but in some areas – and fundraising is one – you will have to decide whether you are going to ask for the consent of the Data Subjects or use their data without consent because

it is *necessary* in your 'legitimate interests'.

There is a caveat: your legitimate interests must not override the 'interests or fundamental rights and freedoms of the Data Subject which require protection of personal data'.

If you are processing data because of your legitimate interests the Data Subject can tell you that they have a particular reason for not wanting you to do so and you would then have to prove that you have 'compelling' grounds for continuing.

Note also that, if your processing is based on legitimate interests you have to be very careful about extending your use beyond the original purpose, and GDPR sets out a number of factors to take into account.

GDPR asks you to take account of people's 'reasonable expectations' in deciding the balance between your interests and theirs.

Action:
Be sure that you know – and can justify – the basis of all your processing, especially if you are relying on legitimate interests.

Transparency

It has always been a key element of Data Protection that people should know enough about what is being done with their data. **'Enough' is now much broader under GDPR**.

The full list, in brief, of information that may have to be made available is as follows (existing DPA requirements are in *italics*, information that must **always** be provided is in **bold**):

- ***the identity and the contact details of the controller***;
- ***the purposes* as well as the legal basis of the processing**.
- **where relevant the legitimate interests**;
- ***any recipient(s)*;**
- **any overseas transfers**;
- the storage period or criteria for deletion;
- right of access;
- right to rectification or erasure;
- right to withdraw consent at any time if processing is based on consent;
- right to complain to the ICO;
- whether the provision of personal data is [contractually] required, as well as whether the Data Subject is obliged to provide the data and of the possible consequences of failure to provide such data;
- whether you are carrying out automated decision making, including profiling.

My understanding is that this information has to be presented using the 'layered approach' that is in the Information Commissioner's current guidance on Privacy Notices, Transparency and Control, which was updated on 7th October 2016 to take account of GDPR.

This means that the key points have to be presented to people at the time they give their information, either on the form or verbally, while the full details are put in an accessible and understandable privacy policy or statement.

What is not clear at the moment is how much information has to be provided up front, and in how much detail. The danger, of course, is that we could end up with a whole raft of unreadable small print on every data capture form, which would not achieve the objective.

Action:
Carry out an exercise to document what you do with personal data in detail and work out how best to explain this to your Data Subjects in a full privacy statement.

Action:
Write a set of appropriate short privacy notices – based on your full privacy statement – for use in different situations and ensure that they are used consistently across your organisation.

Data Subject rights

Many existing rights are retained or enhanced in GDPR, and **there are some new ones**. Here is a selection:

Subject Access

The right is retained, but it will no longer be permitted to charge a fee, and the time limit is reduced from 40 days to a month.

Rectification

The Data Subject can have incorrect data corrected and incomplete data completed.

Erasure ("right to be forgotten")

The Data Subject can tell you to erase their information and you must do so unless you have a good reason (from among the options set out in GDPR) to retain it.

Restriction of processing

The Data Subject can restrict your processing of their data if there is an unresolved question of its accuracy and in some other specified situations.

Portability

In certain cases (mainly where the Data Subject has signed up to online services) they can have their data transferred directly to another provider.

Direct marketing

As now, the Data Subject has the right to stop you from sending them any direct marketing and you must make sure they know about this right.

Profiling & automated decision-making

There has been a lot of debate about 'profiling', stemming from the references to various practices in the Information Commissioner's penalty notices against 13 charities around the start of 2017.

It is not really clear whether GDPR only applies to the kind of profiling that leads to *automated* decisions ("computer says no") or whether it also includes activities fundraisers might carry out in order to decide who to approach and how best to approach them.

GDPR certainly gives people the right in some cases to prevent "*a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*"

Complaints and compensation

Data Subjects have the right to complain to the 'supervisory authority' – i.e. the Information Commissioner – and have the complaint investigated.

They also have the right to take action against a Controller *or Processor* (that's new in GDPR) who is not complying with their Data Protection responsibilities.

As now, Data Subjects have the right to obtain compensation for damage if Data Protection has been breached. GDPR specifies "*material or nonmaterial*

damage", whereas the DPA provides for 'damage and associated distress'. I'm not clear yet what the difference is.

Action:
Make sure you are aware of all these rights and find out more about any that might affect your processing.

Children

GDPR is particularly concerned to **protect children online**. In the UK the government intends to set the age limit for this at 13.

The underlying approach is set out in Recital[1] 38:

> *Children merit specific protection … as they may be less aware of the risks [etc]. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.*

Children's rights are given special attention at various points, such as: ensuring that privacy notices aimed at children are easy for them to understand; rights to correct or remove data given as a child; and getting the right balance on 'legitimate interests'.

Where children are being provided with 'information society services' parental consent must be given if the child is under age, and you must make 'reasonable efforts' to verify that this is genuine.

As far as I understand it, 'information society services' pretty much means any online service, including shopping, social media, mobile apps and the like.

Note that parental consent is not required where you are offering '*preventive or counselling services*' directly to a child.

Action:
If you provide any kind of services directly to children, ensure that you understand what you need verifiable parental consent for and check that your privacy notices are sufficiently easy to understand.

Section 2: Managing Data Protection under GDPR

A significant change in GDPR is that all organisations are now required to be much more systematic in how they manage their Data Protection compliance.

Keeping records

GDPR requires you to take appropriate technical and organisational measures to comply and, importantly, to be able to ***demonstrate* that you are complying**.

There has been no guidance on the type of records you will have to keep, in order to demonstrate compliance, but some of the obvious ones are likely to include:

- Board meeting minutes when Data Protection has been discussed;
- policies relating to Data Protection (including IT security, for example);
- written procedures and guidance for staff to follow;

[1] EU Regulations are divided into 'Recitals' which explain what they are trying to achieve, and 'Articles' which set out the actual rules.

- records of staff induction and training – who, what and when;
- records of any monitoring, audits or reviews aimed at checking that policies and procedures are fit for purpose and being followed;
- records of incidents, how they were handled and what was learned;
- Privacy Impact Assessments (see below).

In addition, GDPR sets out a list of basic information that you must hold, including:

- The purposes of your processing
- The types of Data Subject you have
- The types of Personal Data you use
- Recipients you will disclose the data to
- Any overseas transfers
- Retention periods, where possible
- A general description of your security measures, where possible

Action:
Start maintaining a set of relevant records. Don't leave it until May 2018, because any decisions or actions you take now will affect your future data processing.

Data Protection by design and by default

Data Protection has never been something you can 'bolt on' afterwards, but GDPR makes this explicit. Your systems and procedures must ensure that you **only hold the data you genuinely need for each specific purpose, use it appropriately, and restrict access**.

It is particularly important that you think these things through when you are starting a new activity or setting up a new system.

Action:
Make sure that everyone responsible for starting projects or setting up systems is aware of the need to incorporate Data Protection as a matter of course. Make Data Protection a standard check point before any project or system is signed off.

Relations with other organisations

If you process personal data as part of work in collaboration with other organisations then both or all organisations are likely to be joint Controllers.

In this case GDPR requires you to set out '*in a transparent manner*' your respective Data Protection responsibilities and to make the 'essence' of the arrangement available to your Data Subjects.

Note that, regardless of your agreement, the Data Subjects may exercise their rights against any of the joint Controllers.

Action:
Review all your collaborative projects and activities to ensure that, where applicable, your agreements are clear on each party's Data Protection responsibilities.

Data Processors

GDPR requires you to use only Processors who will '*meet the requirements*' of the Regulation. The **Processor can be held directly responsible** for noncompliance, and this extends not just to security, but to all the Principles.

It is still the Controller's responsibility to select a suitable Processor, and to have a contract with them that contains a large number of specific provisions – most of

which have long been good practice, but which are legally required under GDPR.

Action:
Make sure you can identify all Data Processors your organisation uses, and review your contracts against the GDPR list of matters that must be covered.

Security

Although you have to take measures to ensure compliance with all the Principles, **GDPR makes some specific provisions about security**.

Great importance is place on 'data minimisation' – not holding more data than you absolutely need – and on reducing risk by anonymisation or 'pseudonymisation' where possible. The latter means removing details that would allow other people to identify the individual, even if you have a key somewhere that would allow you to reinstate the identification.

GDPR also makes an explicit link to the standard security concepts of confidentiality, integrity, availability and resilience, and sets an expectation that your security measures will be tested at appropriate intervals.

Action:
If your current security measures are fit for purpose, you are unlikely to need to do much more. However, it would be worth reviewing these to ensure they are up to date with the latest technology and threats.

Breach notification

GDPR introduces a requirement that, if you have a data breach, you must **notify the ICO within 72 hours** (or explain why you are late) unless it is '*unlikely to result in a risk to the rights and freedoms of natural persons*'.

If the breach is likely to result in a *high* risk to people's rights and freedoms you must also notify the individuals affected.

There are various exceptions, and a list of what must be in the notification.

Action:
Make it clear to your staff (and volunteers) that, while anyone can make a mistake, failing to report a breach (or potential breach, or near miss) immediately to the relevant person in your organisation will be treated as gross misconduct. Otherwise you run the risk of not finding out about a breach quickly enough to meet the 72hour deadline.

Data Protection Impact Assessments

Under GDPR you must **undertake an impact assessment** before engaging in any processing that is likely to result in a *high* risk to people's rights and freedoms. This is particularly likely to apply to extensive automated processing and largescale use of special categories of data.

Action:
Make relevant staff aware of the situations when an impact assessment is likely to be required.

Data Protection Officer

There are certain situations where GDPR requires an organisation to **appoint a Data Protection Officer**. It also sets out rules about the DPO being independent, being involved in certain decisions, having appropriate expertise and

reporting to the 'highest management level'.

This arrangement is mandatory for public bodies and for others organisations that are monitoring Data Subjects on a large scale or processing special categories of data on a large scale. Few charities or voluntary organisations are likely to meet this threshold.

However, it is hard to see how any organisation can comply with its new obligations to manage Data Protection effectively unless it puts someone in charge. There is no obvious location for the role, although organisations with a compliance and risk function often locate Data Protection within that remit.

Issues to consider include:

- The DP Lead must be able to cover the whole organisation, not just a specific part (such as client services, IT or fundraising).
- The DP Lead must have enough time to do the job properly.
- The DP Lead must be able to report to the Board when necessary.
- The DP Lead must be able to work with operational managers to ensure that Data Protection is effective in all areas.

Action:
Review the DP role in your organisation and make changes if necessary.

Transfers abroad

The rules on transferring data to other jurisdictions remain much the same.

The main issue will be whether the UK is judged to have 'adequate' Data Protection after it leaves the EU. Without that, EU-based organisations will be restricted to meeting one of the alternative provisions before they can transfer personal data to the UK.

Action:
Note the new requirement described above for Data Subjects to be informed if their data is being transferred abroad. Make sure you know where all your data is being stored or processed.

Fines and enforcement

Under GDPR, each country is obliged to have an independent supervisory authority – the Information Commissioner in the case of the UK.

There is no provision in GDPR for Controllers to register with the supervisory authority (which would mean no income stream for the ICO), but there is an obligation for the government to 'ensure' that the supervisory authority is provided with the necessary resources. In the UK, this will be achieved by retaining the registration (and payment) requirement.

There is an extensive section of GDPR devoted to ensuring effective cooperation between the supervisory authorities across the EU, and the ICO is keen to continue this cooperation.

There has been considerable publicity about the new levels of fines that the ICO will be able to impose. These now rise to €10million (or 2% of global turnover, whichever is higher) for some types of breach and €20million (or 4% of turnover) for others.

The ICO has issued a statement reassuring everyone that she has no intention of significantly increasing the general level of fines she imposes. The clear intention of GDPR is that the higher

amounts should only be applied to very large – probably multinational – companies for whom the current levels of fine are little deterrent.

The Information Commissioner is in the process of developing guidance on GDPR, and has set out her strategy. Guidance is also being produced at the European level, and the ICO will integrate this into its guidance.

So far, the following guidance has been issued *or promised* (see links in the ICO strategy paper):

- Overview of GDPR (ICO)
- 12 steps to take now (ICO)
- Readiness for GDPR checklist (ICO)
- Privacy Notices code of practice (ICO) – *updated to take account of GDPR*
- Data Processor (ICO consultation)
- Data Protection Officers (EU)
- Data Portability (EU)
- Data Protection Impact Assessment (EU)
- Consent (ICO) – *December 2017*

Action:
If you have not already done so, sign up to the Information Commissioner's monthly newsletter, so that you find out when guidance and statements are made and bookmark the ICO's pages on GDPR.

Section 3: Background

This section gives a bit of history, and explains what still has to take place before we have the full story.

How we got to where we are

In January 2012 the EU began considering a replacement for its 1995 Data Protection Directive (95/46/EC). After consideration at length by the Commission, the Council and the Parliament, the new **General Data Protection Regulation** (2016/679) was agreed in December 2015 and signed off in May 2016. This triggered a two year run in period before the Regulation comes into force on 25th May 2018 (at which point the UK will still be part of the EU).

The Regulation is intended, broadly, to achieve three things:

- To take account of technological developments that have taken place since the 1995 Directive was written.
- To remedy areas in which the existing legislation is felt to be unsatisfactory.
- To bring more consistency on Data Protection across the EU.

The fact that this is a Regulation, not a Directive, is the main way in which the last of these is to be achieved. Whereas a Directive instructs national governments to draw up their own legislation, a Regulation applies directly to all EU countries.

What about Brexit?

The UK Government intends GDPR to remain substantially in place even after the UK has left the EU. It would make life very difficult for many UK businesses if our legislation was deemed by the EU not to provide 'adequate' data protection (i.e. equivalent to GDPR).

The UK Government published a **Data Protection Bill** in September 2017 which, among other things, makes a limited number of national variations that are allowed by GDPR and paves the way for GDPR to become part of UK legislation.

Bear in mind that some of what I have said above may have to be modified in the light of the UK legislation.

Another complication: PECR

Alongside the current Data Protection Act the Privacy & Electronic Communications Regulations 2003 (PECR) impose additional restrictions on some direct marketing.

In January 2017 the EU published a proposed overhaul of this legislation, which was supposed to take effect at the same time as GDPR. Progress on this appears, however, to have been slow, and it must now be doubtful whether the deadline will be met.

This could affect issues such as whether there are any circumstances in which you can carry out email or phone marketing without consent. (Some direct marketing by mail is likely to remain permitted without consent as a 'legitimate interest'.)