A not-for-profit Guide to The General Data Protection Regulation or GDPR (EU) and The Data Protection Act 2018 (UK)

Table of Contents

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

Not-for-profit Guide to General Data Protection Regulation or GDPR (EU) and The Data Protection Act 2018 (UK)

1 The new Data Protection Act

The GDPR applies to any business or public body that stores or processes the data of EU residents. This includes every employer in the EU, businesses that offer products and services to EU citizens and residents, and companies that process personal data on behalf of other organizations. The new legislation replaces the Data Protection Act, 1998 prescribing how you as an organisation and your staff manage the **personal data** of your donors, service users, beneficiaries, stakeholders and anyone else working with your organisation.

1.1 The definition of "Personal Data"

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

1.2 Examples of "Personal Data" you may be processing

Employee records, donor mailing lists, membership databases, even your visitors book.

2 How to comply with the GDPR

2.1 Appoint a Data Protection Officer

One of your staff will need to take responsibility for compliance, to do this they need to be given the authority to do so effectively and they need to train in the knowledge required to maintain compliance. The following guide will give them the basics and the tools to answer compliance questions from your staff.

2.2 Organize an information audit

To comply with the GDPR's accountability principles, you need to know your data well. Document what personal information you hold, where it resides, where it came from whom you share it with and your purpose in processing it. You need to know precisely what regulated information you hold and document the risks involved to the data subjects in the event of said data being compromised.

2.3 Identify the legal basis for processing any personal data

Document and explain the legal basis for processing the personal data. You must maintain documentation of the legal bases with regard to all types of information. If your legal basis is explicit agreement (consent) you must have documented evidence that consent was given and that the request for consent is clear and concise.

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

2.4 Be prepared to uphold your subject's rights

Individuals have certain rights that you must uphold, such as the right to access their personal data (called a Subject Access Request or SAR), the right to correct inaccuracies, and the right to have personal information erased. You need to make sure that you have procedures in place to address such requests from data subjects promptly.

2.5 Notify your subjects

You will need to let your subjects know what data you hold about them and update your Privacy Policies to suit the new legislation. Whenevr you collect data you will need to explain clearly to subject why it is being collected and for what purpose it will be used.

2.6 Protect the data

Ensure that the sensitive data is stored in a way that only those of your staff who need to have access to it. Also ensure that you or your IT Support company have a compliant Data Protection Policy in place, covering security, retention, breach notification procedures and backups.

2.7 Apply the eight principles of Data Protection

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

3 The eight principles of data protection

A copy of the full legislation can be found here: https://gdpr-info.eu/

3.1 Ensure you act lawfully

"Personal data shall be processed fairly and lawfully"

3.1.1 In Practise

You must:

1. have legitimate grounds for collecting and using the personal data;
2. not use the data in ways that have unjustified adverse effects on the individuals concerned;
3. be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
4. handle people's personal data only in ways they would reasonably expect;
5. and make sure you do not do anything unlawful with the data.

3.1.2 Choosing a lawful basis

You need to choose at least one lawful basis (**a-f**) to process personal data. Identify one of the following bases and ensure it can reasonably be applied to your use.

In every case you need to document which basis you have applied and keep a record of it.

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

This may apply for example for solicitations for support from donors, or for invitations to events. To comply you will need to obtain **specific consent** from individuals to collect and use their personal data for this purpose. Be transparent about what the data consists of, how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;

The GDPR standard for consent is very specifically "opt-in". You can't use pre-ticked boxes to obtain consent and you need to very clear about what they are consenting to. You also need to be clear that they can opt-out at any time and give clear instructions on how to do so. Keep a record of how you obtained this consent and when.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Cases where this might apply might be for instance event bookings, where an individual can reasonably expect you to store and process data necessary for you to fulfil your role as event organiser.

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

This seems to be the most flexible definition, but you need to be able to prove that you have **legitimate grounds** for collecting and using the personal data;
Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance.

3.1.3 Special Case Categories

Be aware of working with "Special Category" data. The GDPR says these types of data need extra protection, so if you want to process any of the following data you will need to prove that you have special reasons for doing so, and take extra steps to ensure the data is protected.

• ethnic origin;
• race;
• politics;
• religion;
• trade union membership;
• genetics;
• biometrics;
• health;
• sex life; or
• sexual orientation.

3.2 Have a specific purpose

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes"

3.2.1 In practise:

- be clear to subjects about why you are collecting personal data and what you intend to do with it;

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

3.2.2 What does "fair" or "incompatible" mean?

Inviting a database of people who attended an event to another event of similar nature is likely to be compatible with the original purpose for which you gathered the data. Soliciting the very same database for donations however might be considered "incompatible" or "unfair" to the data subject.

3.3 Adequate and relevant

"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed"

3.3.1 In Practise:

- you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual;
- and you do not hold more information than you need for that purpose.

3.3.2 Practise data minimisation

To comply here you should identify the minimum amount of personal data you need to properly fulfil your purpose. You should hold that much information, and no more.

3.4 Accuracy and maintenance

"Personal data shall be accurate and, where necessary, kept up to date"

Don't miss "where necessary", obviously if you have a database that is currently in use, you are obliged to keep it updated and accurate in order for it to stay fit for purpose. If a database is out of use, you do not need to maintain it.

Keeping unused databases however can mean extra work complying with #6 (responding to subject access requests), which you will have to do whether or not the information is accurate.

3.4.1 In practise:

You should:

- take reasonable steps to ensure the accuracy of any personal data you obtain;

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information;
- consider whether it is necessary to update the information.

3.5 Retention

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"

Where personal data is held for more than one purpose, there is no need to delete the data while it is still needed for any of those purposes. However, personal data should not be kept indefinitely "just in case", or if there is only a small possibility that it will be used in future.

3.5.1 In practise

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes;
- update, archive or securely delete information if it goes out of date.

3.5.2 Anonymising data

You may have invested heavily in some information, such as in a detailed survey the data from which could be used for as yet unknown purposes and for this reason you might like to keep the raw data. You can maintain compliance by removing any PII (personally identifiable information), even without which you will still be able to extract useful statistical information from the database.

3.5.3 Audits

A policy of regular data-audits appear to be the focus of compliance in this principal, such audits should assess:

- the current and future value of the information;
- the costs, risks and liabilities associated with retaining the information;
- the ease or difficulty of making sure it remains accurate and up to date.

3.5.4 Special case - shared information

Where personal data is shared between organisations, those organisations should agree about what to do once they no longer need to share the information. In some cases, it may be best to return the shared information to the organisation that supplied it, without keeping a copy. In other cases, all the organisations involved should delete their copies of the information.

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

3.6 The subject's rights

"Personal data shall be processed in accordance with the rights of data subjects under this Act"

The rights of individuals that it refers to are:

- a right of access to a copy of the information comprised in their personal data (**SAR**);
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for **direct marketing**;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
- a right to claim compensation for damages caused by a breach of the Act.

The first and third elements will be the most common encountered, so these should be explained further.

3.6.1 Subject access request (SAR)

A subject access request requires that within 1 month of their request:

- you inform an an individual whether any personal data is being processed;
- give them a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

3.6.2 Verification

The Act allows you to confirm two things before you are obliged to respond to a request. First, you can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception. The second thing you are entitled to do before responding to a subject access request is to ask for information that you reasonably need to find the personal data covered by the request. Again, you need not comply with the subject access request until you have received this information. In some cases, personal data may be difficult to retrieve and collate. However, it is not acceptable for you to delay responding to a subject access request unless you reasonably require more information to help you find the data in question.

3.6.3 Fees

The SAR service needs to be provided free, and if a request is considered "manifestly unfounded or excessive", you can charge a maximum fee of £10. Although you need not comply with a request until you have received a fee, you cannot ignore a request simply

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

because the individual has not sent a fee. If a fee is payable but has not been sent with the request, you should contact the individual promptly and inform them that they need to pay. Provided you have done so, the 1 month period for responding to the request does not begin to run until you have received the appropriate fee and any additional information that is necessary

3.6.4 Reducing risk

Clearly any organisation holding data is exposed to the risk that administration work servicing SAR's can be massive. This risk can be reduced by implementing stricter policies under principle #5 such as deleting or anonymising data rather than archiving it.

3.6.5 Preventing direct marketing

"Individuals have the right to prevent their personal data being processed for direct marketing. An individual can, at any time, give you written notice to stop (or not begin) using their personal data for direct marketing. Any individual can exercise this right, and if you receive a notice you must comply within a reasonable period."

Direct Marketing includes communications by ANY means, for example: letter mailshots, emails, faxes or SMS. It includes the promotion of particular viewpoints or campaigns.

3.6.6 How to respond to Prevent Requests

You do not need to respond directly to the individual (although it may be good public relations to do so), but you you need to take action within 28 days. The industry standard is simply to prevent their systems from including that individual in marketing, but you need to delete their personal information if they request that you do so.

3.7 Data must be protected

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

3.7.1 In practise

Ensure that:

- only authorised people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority;
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

3.7.2 Compliant IT systems

Some of the data protection aspect Principle concerns your IT systems and the IT support you receive from Comm-tech. In this vein we have always designed our clients' systems and support packages to:

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

- Protect data against theft via the internet using security patching, server monitoring, firewalls and other security tools such as antivirus to help prevent security breaches arising from malware infections. We apply additional protection proportionate to the sensitivity of the data our client holds.
- Support granular file sharing, so that management can ensure staff only have access to data that within their employment remit.
- Provide robust backup systems to ensure damaged or deleted data can be recovered, along with SLA's to ensure business continuity is least affected by systems failures.

To this end we also:

- Provide installation services to ensure that new IT equipment is set up in a secure way that protects against security breaches arising from manufacturer default consumer focussed (usually inappropriate) setups.
- Provide advice on compliant disposal services to ensure data is not harvested from discarded IT equipment.
- Ensure that our staff are vetted to the maximum feasible and remain under strict NDA.

3.7.3 Security policies

IT systems that are too proscriptive about the way staff can operate may end up restricting staff in their ability to function efficiently, which may result in subversion. However IT systems that are too flexible can also be subverted, particularly from within. A middle ground is necessary, where some aspects of data protection responsibilities are assumed by staff.

To facilitate this an organisation should show due diligence with regard to their IT security by assigning clear responsibilities and adopting a written IT security policy. The minimum required is as follows:

- be clear about who in your organisation is responsible for ensuring information security;
- do periodic checks to ensure that the organisation's security measures remain appropriate and up to date;
- include in the security policy a clause that limits access to personal information to those who's roles make it necessary to have such access;
- include in the security policy a clause that limits access to premises or equipment given to anyone outside the organisation;

3.7.4 Staff training

Ensure that staff understand the importance of protecting personal data, are familiar with your organisation's security policies, and that they are trained to practise said security policy.

In addition to familiarising staff with the Security Policy wording, training should cover:

- inadvertent mishandling of data, such as the practise of emailing personal data, or failure to encrypt portable media such as USB sticks or laptops (an encryption policy should be in place for all portable media)
- your organisation's duties under the Data Protection Act and restrictions on the use of personal data;

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

- the responsibilities of individual staff members for protecting personal data, including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority;
- the proper procedures to use to identify callers; the dangers of people trying to obtain personal data by deception (for example, by pretending to be the person whom the information is about or by making "phishing" attacks) or by persuading you to alter information when you should not do so;
- any restrictions your organisation places on the personal use of its computers by staff (to avoid, for example, virus infection or spam).

3.8 Where the data can be stored

"Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

Other than EEU countries the only ones who are certified to protect data adequately are: Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland Uruguay. At this time Canada is also considered partially adequate.

3.8.1 In Practise

Ensure that you do not store personal data in countries outside the EEU apart from those considered "Adequate" above. When assessing compliance take into account the following:

- the nature of the personal data being transferred;
- the country or territory of origin of the information in question;
- the country or territory of final destination of that information;
- how the data will be used and for how long;
- the security measures to be taken in respect of the personal data in the country or territory where the data will be received.

Most of our clients host their data either in their own offices or in our cloud systems which are hosted only in the UK. Those using Microsoft Office365 or Google For Business will have chosen in which countries the provider is allowed to store that data.

When using 3rd party Apps such as image-to-pdf, photograph processing, think about the implications first. Where (in terms of compliance) is the data going for processing and why?

205 Amesbury Ave
London SW2 3BJ
www.comm-tech.org
0208 671 5555

4 Further help

COMM-TECH are providing an ongoing GDPR support service to assist our client DPO's. Please contact privacy@comm-tech.org to arrange time with us. The service is supplied on an hourly basis at Project rates.

5 Disclaimer

*** ***

The information in this document is issued to our clients as part of our support services only and is not intended to be, nor does it constitute, legal advice

*** ***

If you have any questions, please email privacy@comm-tech.org and we'll do our best to advise.

COMM-TECH.ORG, May 2018