GDPR: Data Protection

The UK's first Data Protection Act was passed in 1984 and the second Act was passed in 1998, coming into force on 1 March 2000. The General Data Protection Regulation (GDPR) was passed in
2016 and comes into force after a two-year preparation period on 25 May 2018. GDPR originated in the European Parliament but will be fully absorbed into UK law regardless of the UK exiting the European Union. The regulation will apply across all EU member states including the Republic of Ireland, where it replaces the Acts of 1988 and 2003.

This is the most significant update of data protection laws in some time and has, understandably, lead to much confusion and misinformation across the voluntary sector. This Briefing will help you understand your obligations and cover all the basics of GDPR in plain English.

Why do we have data protection laws?

Data Protection laws arose from concerns over individuals' right to privacy as increasing amounts of personal information was gathered by businesses and other organisations throughout the 20th century.

Digital technology has changed the way many organisations operate and the evolving means of collecting, storing and processing personal data has meant that laws have needed to be significantly changed to keep pace. GDPR takes account of modern methods of capturing and processing people's data and takes steps to ensure individuals have sufficient control over their information.

It is important to remember though, that data protection isn't just about digital information but all personal information, including that which is recorded or stored in paper copies.

Who does GDPR cover?

GDPR, like previous legislation, is aimed at protecting individuals, not organisations. Named individuals in the workplace are also covered where their personal information is concerned. The principles of GDPR are therefore easier to understand if you consider them from the point of view of a member of the public.

Organisations, including businesses and charities, are liable for their breaches of data protection laws, even if the breach is the action of an individual. With a significant increase in the level of fines that can be imposed – as well as changes in the rights of individuals – it is crucial for organisations to ensure that their staff and volunteers understand their responsibilities when it comes to gathering, storing and using personal data.

How does it affect us?

GDPR details procedures that are required by law, so your organisation needs to adhere to these to be compliant and avoid a fine from the Information Commissioner's Office and, potentially, a compensation claim on behalf of those individuals affected. It is therefore essential to make sure that you are following best practice in terms of the following:
How you gather information
How securely you store information
How you comply with reasonable requests for the information
you hold
How you can evidence any of the above in the event of an audit

Ensuring that you have clear policies and acceptable processes in place will give you a strong case against a hefty fine in the event of a breach or audit.

Types of Data:

Personal Data
This is any information which relates directly to an individual and can be linked directly to them. For example, this includes: name, phone number, email address, photographs, genetic and economic data. This kind of data is the focus of GDPR and data protection.

Anonymous Data
Data which has been anonymised properly cannot be traced back to the original individuals in any way but can still be processed by organisations to conduct research. Fully anonymous data is not covered by GDPR as it contains no personal information to protect.

Pseudonymous Data
Some data, which has been properly pseudonymised, can only be connected back to an individual using a specific 'key' or code. This can be an extra layer of security but the data is still treated as Personal Data under GDPR because of the possibility of personal identification.

Changes to Data Protection Act (1998)

Much of the coverage of the changes brought in by GDPR has focused on the large fines but, in practice, some of the most significant changes that will affect how we all work is in the additional rights afforded to individuals. These allow individuals to request access, corrections and removal of their personal information in ways that weren't available before.

The new regulation requires clearer evidence of consent from individuals and some methods of recording consent will no longer be valid. Additionally, GDPR gives greater powers to the ICO (Information Commissioner's Office) to investigate organisations and breaches.

Definitions

- Data subject – This is a term used to refer an individual whose personal information is the data in question.
- Processing – This refers to the collection, storing and
- transferring of personal data.
- Profiling – This is something that is often done by larger organisations and involves automatic processing of personal information (often in large batches) to evaluate aspects of the individuals' behaviour and make decisions or take actions.
- ICO – The Information Commissioner's Officer is the UK's independent authority set up to uphold information rights in the public interest. In the Republic of Ireland, the Data Protection Commissioner holds a similar position.
- Data Controller – This is the person within an organisation that
- decides what data is collected, used for and who it is shared with.
- Senior Information Rights Owner (SIRO) – This is usually a
- board level role to oversee data policies.
- Data Protection Officer – This role is required in certain circumstances, such as public authorities and those organisations dealing with sensitive data.
- Data Processor – This refers to anyone, sometimes a third-party organisation or business (eg. printing company), who processes data on the instruction of your Data Controller.
- Principles of GDPR

GDPR legislation lays out six principles for processing of personal data. These are:

Lawfulness, fairness and transparency

This covers the primary areas of concern that data should be gathered and used in a way that is legal, fair and understandable. The public have the right to know what is being gathered and have this corrected or removed.

Purpose limitation

Organisations should only use data for a legitimate purpose specified at the time of collection. This data should not be shared with third parties without permission.

Data minimisation

The data collected by organisations should be limited only to what is required for the purpose stated. Organisations should not collect data in mass without purpose.

Accuracy

The personal data you hold should be accurate, kept up to date, and, if it is no longer accurate, should be rectified or erased.

Storage limitation

Personal data should only be stored for as long as is necessary. Data can be archived securely and used for research purposes in the future. Where possible, the personally identifiable information should be removed to leave anonymous data.

Integrity and confidentiality

Personal data should be held in a safe and secure way that takes reasonable steps to ensure the security of this information and avoid accidental loss, misuse or destruction.

What to do

Audit

If you have not done so recently, it is advisable to undertake a full audit of the data you may hold in your organisation. Try to think of different ways that people may have captured personal information and where this would have been recorded or stored. This includes paper and digital records.

Once you've gathered and assessed all of the personal information you hold, you should decide whether you still need it and, if not, delete it. For the data you hold and would like to retain, you will need to be able to demonstrate reasonable consent from individuals to do so.

Consent

There are six valid reasons for processing personal information or communicating with an individual. These are known as 'conditions for processing' and include legal obligations and actions which are necessary for completion of a contract. Most commonly – outside of commercial and legal operations - you will probably be using 'consent' as your condition.

Under GDPR, consent from individuals must be affirmative, freely given, specific, informed and unambiguous. This means that they must actively give consent for their data to be processed. Silence, inaction and pre-ticked boxes are not valid as consent.

During an investigation by the ICO, you may be asked to show how and when consent was granted, so it is vital that you record this and can provide evidence. This might be as simple as holding copies of forms where a box has been ticked or having digital records of when the user opted in to share their data.

Privacy statements

A clear, simple privacy statement should be available at the time that an individual gives their consent to share personal data.
This should be as brief and simple as possible to ensure that individuals can reasonably understand the purpose of collection. You should avoid having broad, catch-all notices and instead have specific notices for different purposes. It is important to offer individuals clear information, choice and control over their data. At the point of gathering personal data, you are required to provide certain information including:

- the identity of the Data Controller (and Data Protection Officer, if applicable),
- the purpose of collection,
- whether any sharing with third parties or international transfers
- will take place,
- how long the data will be held,
- the details of the individual's rights regarding the data (see p4)
- notice of any automated decision-making ('profiling') that may take place using the data

This information can be included within the privacy notice at
the point of giving consent or, at the latest, included in the first contact you have with the individual. Remember that the option to opt-out must always be available and should be included in any communications with the individuals.

Roles

You should decide on an appropriate individual to be your organisation's Data Controller. They should carefully consider all aspects of GDPR in planning and storing any personal information and should be available and contactable to handle any requests.

If you have a board, you should also have a member of the board identified as SIRO (Senior Information Rights Owner) to set and approve formal policies and ensure the Data Controller is given suitable guidance and is following this correctly.

Appointing a Data Protection Officer is only required if you are a public authority, if you carry out large-scale systematic monitoring (behaviour tracking) or if you carry out large scale processing of special categories or data relating to criminal offences. Think about the work your organisation does and if it fits in these categories. If it does, you may need to appoint a DPO in addition to the above roles.

Retention policy

Any data you hold should only be kept for as long as it is necessary and useful. You should not hold personal information indefinitely unless there is a valid reason for this. Your organisation should agree a Data Retention Policy that considers the kind of data you collect, how you use it and when this data should be reviewed or deleted. This could be a review every two years, for e
your data and keep only what is relevant and current.

Your Data Retention Policy should suit your activities and can be short and straightforward but should always consider any other legal requirement to maintain records. Data should always be deleted if an individual has withdrawn consent, if a contract has been entirely completed or if the data is no longer up to date.
Certain elements of the data can be held indefinitely if these are anonymised (removing personally identifiable data).

Special categories

These categories of personal data have stricter rules regarding their processing, so must be treated carefully. They can be processed *only* with explicit consent to do so, or if it is a necessity in performing a contract. This type of information can, however, be gathered in an anonymised form for the purpose of research and monitoring.

- Racial and ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Data on health, sex life or sexual orientation
- Genetic or biometric data

Rights and requests

Individuals have several rights under GDPR which your organisation must be able to adhere to and be able to respond to requests within the specified times. You *can and should* request valid proof of identification from the individual before proceeding with the request. If you have shared data with a third party, you may have to notify them of changes or deletion. Similarly, a third party may pass on a request from an individual instructing you to alter or delete shared data. The rights of individuals are detailed below:

Right to be informed	Individuals should be informed of how their data is collected, stored and processed in a clear, accessible way	You should provide this in your Privacy Statements and by request
Right of access	Individuals can request access to a copy of their data in electronic form and details of how it is processed	You must provide this, for free, within one month
Right to rectification	Individuals are entitled to have their data corrected if it is inaccurate or incomplete	You should do this within one month, two if it is a particularly complex task
Right to erasure	Also known as 'the right to be forgotten', this permits individuals to request the deletion of their data	You must do this within one month, unless you have a strong, valid reason
Right to restrict processing	Individuals can request a halt on processing if they object to accuracy or purpose but you can still hold the data until resolved	This should be an immediate, and often temporary, stop
Right to data portability	Individuals can request their data in a suitable digital format, sent either directly to them or to a third party	You should do this within one month, two if it is a particularly complex task
Right to object	Individuals can, in certain cases, object to the processing of their data, eg. in direct marketing	You should provide reasonable means to object and act on this within one month
Rights in relation to automated decision making	Individuals can object to potentially damaging decisions being taken against them based only on automated data processing	You should allow the individual to challenge and request human intervention

FAQ's

Children

GDPR enhances the protection of children's personal data. Any privacy notices for services offered directly to a child must be written in clear, simple language to be taken as valid. A child under 16 cannot give consent themselves. This is required from a person holding 'parental responsibility'. There is scope for individual EU member states to legally lower this age, but not below the age of 13.

Breaches

If you suffer a security breach and personal data is compromised, you must notify the ICO within 72 hours. Your report to the ICO should detail what data has been breached (amount, type of data), the likely consequences, the steps already taken to mitigate and the name of your Data Protection Officer. Data that is properly encrypted or anonymised but lost/stolen is not considered a breach as it can't be linked to individuals. If you have good, suitable policies and processes in place, then the breach will be minimal and a fine is unlikely, but if your management of the data has been negligent then the ICO can impose a significant fine. Individuals can also seek
compensation, either through courts or through payment, for the damage incurred.

Mailing Lists

Email newsletters are common among many voluntary groups and organisations so ensuring that this data is being handled correctly is very important. Most groups will manage this through an online service like MailChimp. These companies will have Privacy Policies and other ways of indicating their compliance with GDPR and/or Privacy Shield (see 'International Transfers'). They will usually also record when and how a user was entered into the list so this may be your best means of proving consent.

Remember, all of your emails *must* include an opt-out or unsubscribe link.

Events: photography & filming

Images of people are considered personal data as they can be identified by these images. This means that photographing and filming at events is a form of personal data collection. If you want to store, use or share these images, then you must have clear, active consent from the individuals concerned. As noted previously, silence and inactivity is not permissible as consent so signs at an event that simply notify attendees or require them to state their objection will not count as consent having been given. Draft a simple consent form that all members of the audience can read, understand and sign at the door to give clear consent.

Continue reading on next page

Conclusion

Privacy by design/default

Rather than retrospectively worrying about how to comply with GDPR, it is best for your organisation to adopt a privacy by design or default position. This means taking data protection into account in the early stages of planning a new project or adopting new technologies or systems. It means developing strong privacy policies and Privacy Impact Assessments where necessary. Most importantly, it means that the default position needs to always respect the privacy of the individual and not presume that you have consent to use personal data.

Common sense

Quite a lot of GDPR is based on common sense. It updates the previous Data Protection Act of 1998 to clarify existing principles and strengthen the rights of individuals, including children in the digital age. While the talk surrounding GDPR can sound complicated and scary, always try to think about whether your approach to data makes sense.

Ask yourself simple questions about personal information every step of the way: *Should we be collecting this? Is this useful and accurate? Have we got clear permission to use this? Should we still be holding this? Can we share this? Is our data held securely and safely? Is this request genuinely from the individual concerned? Are the businesses we work with also compliant?*

The 'Principles of GDPR' section mentions fairness and transparency, so try to put yourself in the shoes of the individuals and assess whether your use of their data is fair and if you'd be happy to be transparent about your processes.

Further Resources

Information Commissioner's Office (UK)
Tel: 0303 123 1113 (option 4: Advice for small charities)
GDPR summary
Privacy Impact Assessments

Data Protection Commissioner (Republic of Ireland) Tel: +353 57 8684800
GDPR website

NCVO: KnowHow Non-Profit guide to GDPR Institute of Fundraising: Get Ready for GDPR RefTech: Data Protection in the Events Industry
MailChimp: GDPR: What it is, what we are doing and what you can do