COSCA (Counselling & Psychotherapy in Scotland)
16 Melville Terrace | Stirling |FK8 2NE
t: 01786 475140
e: info@cosca.org.uk: www.cosca.org.uk

General Data Protection Regulation

Information and Guidance for Individual and Organisational Members of COSCA (Counselling & Psychotherapy in Scotland)

1. Introduction

On the Information Commissioner's website, you will find an overall guide to the UK General Data Protection Regulation (GDPR):
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-gdpr/

Individual and organisational members of COSCA (Counselling & Psychotherapy in Scotland) who process data, for example client records, should check whether they are covered by the General Data Protection Regulation (GDPR). You can do this by using the Registration Self-Assessment on the Information Commissioner Office's website, which also checks whether you need to pay a registration fee for processing personal data by clicking on the link below:

https://ico.org.uk/for-organisations/register/self-assessment/

You can assess your compliance with data protection law by using this self-assessment toolkit: Data protection self assessment | ICO

Further help is provided in the link to assess what you need to do to be compliant with data protection legislation:

How well do you comply with data protection law: an assessment for small business owners and sole traders | ICO

As a member of COSCA, if you are covered under GDPR, you should review:

- what you say in your client contract and in your privacy policy about how you will collect and use the personal data of your clients, employees, volunteers etc.
- how and where you keep the personal data of your clients to ensure that it is secure

Charity Registered in Scotland No. SC018887
Charitable Company Limited by Guarantee Registered in Scotland No. 142360

- the amount of personal data you keep on clients and the length of time you keep their records – see COSCA's Guideline on Record Keeping on www.cosca.org.uk under 'ethics'.

The Information Commissioner has a '*Preparing for the GDPR – 12 Steps* ***guide'*** for organisations to assess current practice in specific areas.

It has also a set of guidance and a compliance checklist. See the Information Commissioner Office's website for further information.
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Notification is a statutory requirement and every organisation/individual which processes personal information must notify the ICO unless they are exempt. Failure to notify is a criminal offence.

2. Information on GDPR

The information provided below is offered to members to assist them in understanding and implementing GDPR.

2.1 Useful Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Further information on personal data is given in Appendix A: Personal Data.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

'**Processing**' means almost anything you do with data counts including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

A '**controller**' is the person that decides how and why to collect and use the data. This will usually be an organisation, but can be an individual (eg a sole trader). If you are an employee acting on behalf of your employer, the employer would be the controller. The controller must make sure that the processing of that data complies with data protection law.

A '**processor'** is a separate person or organisation (not an employee) who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller's obligations.

A '**data subject**' is the technical term for the individual whom particular personal data is about.

A '**subject access request (SAR)**' is the Right of Access allowing an individual to obtain records to their personal information, held by an organisation.

A **'privacy notice'** sets out the manner in which personal information is processed**.** You can see and make use of COSCA's privacy notice at the foot of its website. www.cosca.org.uk

2.2 What is the UK GDPR?

The UK GDPR is the UK General Data Protection Regulation. It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context,

As an individual or organisational member of COSCA, you may need to comply with both the UK GDPR and the EU GDPR if you operate in Europe, offer goods or services to individuals in Europe, or monitor the behaviour of individuals in Europe. The EU GDPR is regulated separately by European supervisory authorities, and you may need to seek your own legal advice on your EU obligations.

If you hold any overseas data collected before 01 January 2021 (referred to as 'legacy data'), this will be subject to the European Union GDPR as it stood on 31 December 2020 (known as 'frozen GDPR'). In the short term, there is unlikely to be any significant change between the frozen GDPR and the UK GDPR.

2.3 What is the Data Protection Act 2018?

The Data Protection Act 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

It sits alongside and supplements the UK GDPR - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

The ‘applied GDPR’ provisions (that were part of Part 2 Chapter 3) enacted in 2018 were removed with effect from 1 Jan 2021 and are no longer relevant. The processing of manual unstructured data and processing for national security purposes now fall under the scope of the UK GDPR regime.

The Information Commissioner’s Office’s website states the following about data protection under GDPR and DPA:

- Data protection is about ensuring people can trust you to use their data fairly and responsibly.
- If you collect information about individuals for any reason other than your own personal, family or household purposes, you need to comply.
- The UK data protection regime is set out in the DPA 2018, along with the UK GDPR. It takes a flexible, risk-based approach which puts the onus on you to think about and justify how and why you use data.
- The ICO regulates data protection in the UK. We offer advice and guidance, promote good practice, carry out audits, consider complaints, monitor compliance and take enforcement action where appropriate.

2.4 Who does the UK GDPR apply to?

- The UK GDPR applies to ‘controllers’ **and** ‘processors’.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the UK GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the UK GDPR places further obligations on you to ensure your contracts with processors comply with the UK GDPR.
- The UK GDPR applies to processing carried out by organisations operating within the UK. It also applies to organisations outside the UK that offer goods or services to individuals in the UK.
- The UK GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

3. Data protection principles

HR-related personal data must be processed in accordance with the following 7 data protection principles:

- Lawfulness, fairness and transparency: The organisation processes personal data lawfully, fairly and in a transparent manner.
- Purpose limitation: The organisation collects personal data only for specified, explicit and legitimate purposes.
- Data minimisation: personal data can be processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Accuracy: accurate personal data must be kept and all reasonable steps taken to ensure that inaccurate personal data is rectified or deleted without delay.
- Storage limitation: personal data must only be kept for the period necessary for processing.
- Integrity and confidentiality (storage): appropriate measures must be adopted to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- Accountability: responsibility must be taken for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance.

Individuals must be told the reasons for processing their personal data, how such data will be used and the legal basis for processing it. This should be done in a privacy notice. Personal data of individuals must not be processed for other reasons. HR-related data must not be shared with third parties, except as set out in the privacy notice. Where legitimate interests are used as the basis for processing data, an assessment should be carried out to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where special categories of personal data or criminal records data are processed to perform obligations or to exercise rights in employment law, this must be done in accordance with the Protecting Vulnerable Groups (PVG) Scheme.

HR-related personal data must be up-dated promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment or volunteer relationship or internship is held must be held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which HR-related personal data is held must be contained in the privacy notice issued to individuals.

A record of processing activities in respect of HR-related personal data must be held in accordance with the requirements of the General Data Protection Regulation (GDPR).

4. Lawful Basis for Processing

4.1 Is a lawful basis to process data required?

The ICO states the following:

You must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

You must determine your lawful basis before you begin processing, and you should document it. We have an interactive tool to help you.

Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis.

Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.

If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).

If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

4.2 What are the lawful bases for processing?

The ICO states that:

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

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

(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.

(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 cannot apply if you are a public authority processing data to perform your official tasks.)

5. Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

5.1 Subject access requests

Individuals have the right to make a subject access request (SAR). If an individual makes a subject access request, they must be told:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the member has failed to comply with their data protection rights; and
- whether or not the member carries out automated decision-making and the logic involved in any such decision-making.

The member will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

If the individual wants additional copies, the member can charge a fee, which will be based on the administrative cost to the member of providing the additional copies.

To make a subject access request, the individual should send the member concerned or use the member's form if they have one for making a subject access request. In some cases, the member may need to ask for proof of identification

before the request can be processed. The member will inform the individual if they need to verify their identity and the documents it requires.

The member will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the member processes large amounts of the individual's data, it may respond within three months of the date the request is received. The member will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the member is not obliged to comply with it. Alternatively, the member can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the member has already responded. If an individual submits a request that is unfounded or excessive, the member will notify them that this is the case and whether or not they will respond to it.

5.2 Other rights

Individuals have a number of other rights in relation to their personal data. They can require the member to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the member's legitimate grounds for processing data (where the member relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the member's legitimate grounds for processing data.

To ask the member to take any of these steps, the individual should send the request to the member.

6. Data security

Members must take the security of HR-related personal data seriously. They should have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Examples of such policies are an IT policy on security and confidentiality, Data Retention policy and Register of HR-related personnel data.

Where the member engages third parties to process personal data on its behalf, such parties must do so on the basis of written instructions, be under a duty of confidentiality and be obliged to implement appropriate technical and internal measures to ensure the security of data.

7. Impact assessments

Some of the processing that members carry out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, members will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8. Data breaches

If members discover that there has been a breach of HR-related, client and other personal data that poses a risk to the rights and freedoms of individuals, they must report it to the Information Commissioner **within 72 hours of discovery**. Members must record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, members must tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures they have taken.

9. International data transfers

Members must not transfer HR-related personal data to countries outside the European Economic Area (EEA).

10. Individual responsibilities

Individuals are responsible for helping members keep their personal data up to date. Individuals should let members know if data provided to members changes, for example if an individual moves house or changes their bank details.

Individuals may have access to the personal data of other individuals in the course of their employment, volunteer period or internship. Where this is the case, members rely on individuals to help meet their data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside of member) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the members' premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;

- not to store personal data on local drives or on personal devices that are used for work purposes; and
- **to report data breaches of which they become aware to the member immediately.**

Further details about the members' security procedures should be found in other policies e.g. IT policy on security and confidentiality.

Members should make it clear that failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the members' disciplinary procedure. They should also make it clear that significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

11. Training and Information

Members should themselves be informed of GDPR and provide training/information to all relevant individuals about their data protection responsibilities as part of the induction process and as appropriate thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing the members' GDPR policy or responding to subject access requests under this policy, should be given additional training/information to help them understand their duties and how to comply with them.

Brian Magee
Chief Executive
COSCA (Counselling & Psychotherapy in Scotland)
March 2022

Appendix A: Personal Data

The ICO's website provides the following information about personal data:

'Personal data means information about a particular living individual. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public.

It doesn't need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.

It doesn't cover truly anonymous information – but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data.

It only includes paper records if you plan to put them on a computer (or other digital device) or file them in an organised way. If you are a public authority, all paper records are technically included – but you will be exempt from most of the usual data protection rules for unfiled papers and notes.

Understanding whether you are processing personal data (information that relates to an identified or identifiable individual) is critical to understanding whether the UK GDPR applies to your activities.

What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.

Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.

When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual.

It is possible that the same information is personal data for one controller's purposes but is not personal data for the purposes of another controller.

Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of UK GDPR.

Information which is truly anonymous is not covered by the UK GDPR.

If information that seems to relate to a particular individual is inaccurate (ie it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual'.

The UK GDPR applies to the processing of personal data that is:

- wholly or partly by automated means; or
- the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.

Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

Pseudonymisation (reversible anonymisation): pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

If personal data can be truly anonymised then the anonymised data is not subject to the UK GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.

Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.

Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

What are 'Identifiers and related factors'?

- An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.
- A name is perhaps the most common means of identifying someone. However whether any potential identifier actually identifies an individual depends on the context.
- A combination of identifiers may be needed to identify an individual.
- The UK GDPR provides a non-exhaustive list of identifiers, including:

    - name;
    - identification number;
    - location data; and
    - an online identifier.
- ‘Online identifiers’ includes IP addresses and cookie identifiers which may be personal data.
- Other factors can identify an individual.

- If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable).
- You don’t have to know someone’s name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.
- If an individual is directly identifiable from the information, this may constitute personal data.

- It is important to be aware that information you hold may indirectly identify an individual and therefore could constitute personal data.
- Even if you may need additional information to be able to identify someone, they may still be identifiable.
- That additional information may be information you already hold, or it may be information that you need to obtain from another source.
- In some circumstances there may be a slight hypothetical possibility that someone might be able to reconstruct the data in such a way that identifies the individual. However, this is not necessarily sufficient to make the individual identifiable in terms of UK GDPR. You must consider all the factors at stake.
- When considering whether individuals can be identified, you may have to assess the means that could be used by an interested and sufficiently determined person.
- You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments).

What does ‘relates to’ mean?

Information must ‘relate to’ the identifiable individual to be personal data.

- This means that it does more than simply identifying them – it must concern the individual in some way.
- To decide whether or not data relates to an individual, you may need to consider:
    - the content of the data – is it directly about the individual or their activities?;

    - the purpose you will process the data for; and
    - the results of or effects on the individual from processing the data.
- Data can reference an identifiable individual and not be personal data about that individual, as the information does not relate to them.
- There will be circumstances where it may be difficult to determine whether data is personal data. If this is the case, as a matter of good practice, you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.
- Inaccurate information may still be personal data if it relates to an identifiable individual.

What happens when different organisations process the same data for different purposes?

- It is possible that although data does not relate to an identifiable individual for one controller, in the hands of another controller it does.
- This is particularly the case where, for the purposes of one controller, the identity of the individuals is irrelevant and the data therefore does not relate to them.
- However, when used for a different purpose, or in conjunction with additional information available to another controller, the data does relate to the identifiable individual.
- It is therefore necessary to consider carefully the purpose for which the controller is using the data in order to decide whether it relates to an individual.
- You should take care when you make an analysis of this nature.

Brian Magee
Chief Executive
COSCA (Counselling & Psychotherapy in Scotland)
March 2022