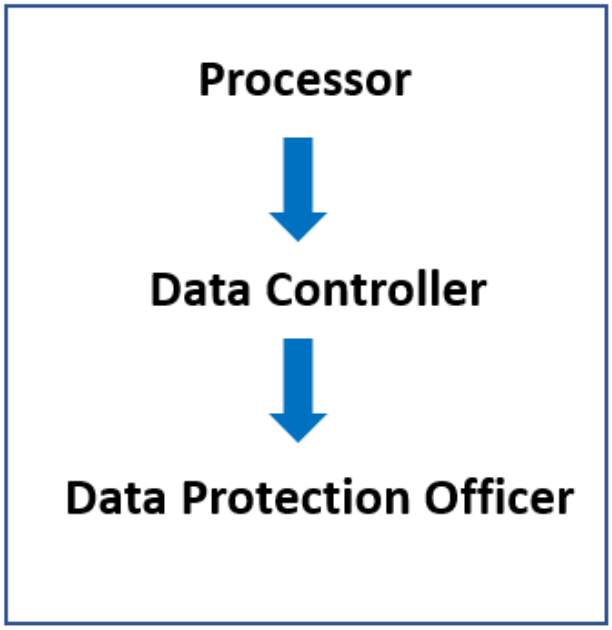
ICTherapies
Inspirational Change

GDPR Compliance Action Plan

June 2020

Table of Contents

Roles and Responsibilities



A **Processor** is responsible for processing personal data on behalf of a Data Controller. It is the responsibility of the **Processor** (e.g. virtual assistant, associate therapist, associate case manager, service provider) to bring a breach in data to the attention of the Data Controller.

A **Data Controller** determines the purposes and means of processing personal data. The **Data Controller** is the legal entity (e.g. Limited Company), where ultimately the Directors are responsible.

The **Data Protection Officer** role can be an in-house position within a company or can be the role of an external person who has solid knowledge and experience of data protection legislation. It would be the responsibility of the **Data Protection Officer** to inform the Information Commissioner's Office (ICO) of a breach.

If there was a data breach it would need to be addressed immediately by the **Data Controller**, through actions of the **Data Protection Officer**. Where no DPO is appointed, an agent (e.g. employee, Director) of the Data Controller must take action.
The **Data Protection Officer** has a window of 72 hours (this is from the time the breach took place) to report the problem to the Information Commissioner's Office (ICO).

The **Controller** retains overall responsibility for the protection of personal data, but the **Processor** has an important role to play to enable the **Controller** to comply with its obligations, this includes breach notification.

The processing of data by a **Processor** shall be governed by a contract or other legal act. The contract must set out the details of the processing and shall stipulate the Processor's duties and obligations, as required by the GDPR.

GDPR Project Team

List of individuals involved in processing business data that contains personal identifying elements.

See also the “Technology Used” page for breakdown of technology service providers who are also Processors under the GDPR.

Data Protection Officer	Not Required – Small Business
Data Protection Champion	Not Applicable
Data Controller	Inspirational Change Therapies Limited Directors: Susana Oppey and Isaac Oppey
Data Processors	None.
Employees and Apprentices *(note that employees do not count as processors under GDPR, but do need to be aware of the regulations in order to assist the Company with compliance)*	None.

Lawful Basis for Processing Data

The first principle requires that you process all personal data lawfully, fairly and in a transparent manner.

Processing is only lawful if you have a lawful basis under Article 6. To comply with the accountability principle, you must be able to demonstrate that a lawful basis applies.

If you are processing special category data (racial, political, religious, union membership, genetic, biometric, health- or sex-related data, or data relating to criminal convictions) you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

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

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

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.

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

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

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.

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.)

If you are relying on legitimate interests to process data, you need more detail in your privacy notices. To read more see this link.

Remote Workers

If you have remote associate team members that live in countries within the EU and work for your company, you will treat them the same as your remote associate team members based in the UK. You will provide them with the same Associate Agreement and Information Notice about GDPR compliancy.

If you have remote associate team members who work for your company, but reside outside the EU, this will have transfer restriction obligations (note these restrictions do not apply to employees). To find more information on this, visit:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

Security Considerations for Mobile Working

There are some excellent guidelines on mobile working on this link below, a list of dos and don'ts for your mobile security policies for the workplace:

https://united-kingdom.taylorwessing.com/globaldatahub/article_security_risk_mobile.html

Some of the items on the list would be ideal for adding to your Data Protection Impact Assessments.

Working with Third Party Providers

If you use a third-party provider to process your client data, they will also need to be GDPR compliant.

It is not always easy to find information as to confirmation of GDPR compliancy, the third-party provider should have information on their website about this. It would be a suggestion to request details of their compliancy before any work takes place.

Data Subject Rights

Information below taken from the ICO website at this link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

It states that the right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. As an example, a privacy notice can be provided on the reverse of a consent form. This is what the Data Subject Rights should cover as below.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The lawful basis for your processing can affect which rights are available to individuals. Some rights will not apply, depending on the lawful basis under which the data is being processed.

Data Mapping

Within your company:

What data is collected? (GDPR Principle 3 – data minimisation)	**Client Information:** • Name • Date of Birth • Gender identity • Sexual orientation? • Ethnicity data? • Contact details (address, email, telephone) • Medical history, lifestyle information, health and wellbeing details • Family/social circumstances • Clinical Reports from other healthcare professionals • Names of key people to the client and their contact details (email, phone), e.g. family members, carers, etc. • Education Provider / Employer details, as applicable • Referrer Details – local authority, solicitors, rehab provider. • Voice recordings (only with consent and when required)
What is your lawful basis for processing the personal data you are collecting? (GDPR Principle 1 – lawful, fair, transparent)	*Article 6 basis for processing:* We primarily process data on the Contract and Legal Obligation bases. For clients, we have a contract in place to deliver psychological therapy services to them for which we require their personal data in order to provide those services. We only collect and process data which is necessary to fulfil our obligations to our clients. We also collect and process client data because it is required by law in order to keep appropriate clinical records. *Article 9/Schedule 1, Condition 2 basis for processing:* Special Category data (health information) is being processed because it is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health care or treatment pursuant to contract

	with a health professional. For new enquiries, these are potential clients who may wish to enter into a contract with us, therefore the data is also being processed under the Contract basis. For any business activities which are not a lawful requirement or essential to the provision of services to the client, we will request their Consent, e.g. for taking audio recordings for the clinician to use for supervision purposes; for sharing the client's clinical reports with a third party; for sending marketing emails. In the event of an emergency (e.g. a client suspected to be harmed/at risk) we may process data, including sharing it without their consent, under the Legal Obligation (safeguarding/duty of care) or Vital Interests basis, in order to protect them. We inform clients of this information via our Privacy Statement as part of, or appended to, our Terms and Conditions. We also have privacy terms for the general public on our website.
Is there an information notice or consent form used to collect the data? (GDPR Principle 1 – lawful, fair, transparent)	A new consent form has been developed to both inform clients of their rights and to obtain consent where this is necessary.
Where is the data stored? (GDPR Principle 6 – integrity)	See pages below "Mapping Business Areas" and "Technology Used" for full breakdown.
What is the data specifically used for? (GDPR Principle 2 – purpose limitation)	Client data is used for the provision of Psychological Therapy services. Specifically: • To identify the client. • to make fully informed recommendations for their treatment. • for communication with the client (or their

	representative) regarding their treatment. • for writing reports. • for sharing data with other clinical professionals, with consent and as required. • for keeping required clinical records. • for safeguarding/duty of care. • for invoicing the client. Client data may be used for Supervision/Accreditation purposes of the clinician and/or for sending marketing emails, but client consent will be obtained for this use.
Who is allowed to access the data? (GDPR Principle 6 – confidentiality)	Only Susana Oppey and Isaac Oppey have access to all client data.
Who is the data shared with externally, third parties? Are contracts in place to manage responsibilities in relation to shared data? (GDPR Principle 6 – confidentiality)	Data is not routinely shared with anyone else other than client themselves. Data (e.g. clinical reports) may be shared with the client's referring party, where this is relevant, but only with client consent. Personal data may be shared with the local authorities/emergency services if it is felt the client or others are at risk of harm (safeguarding/duty of care). This is a legal requirement and does not require consent. When sharing data with medical professionals or appropriate authorities, we are both bound by legal codes of practice in relation to use of personal data.
How and when is the data reviewed, supplemented, updated? (GDPR Principle 4 – accuracy)	Data is reviewed and updated on an ongoing basis, when interacting with the client.

How long is the data kept? (GDPR Principle 5 – storage limitation)	Once a client has been discharged their records are kept for 7 years for adults and 7 years after their 18th birthday for children, unless upon review it is deemed necessary to retain them for longer. If it is the case that data is kept for longer, this is documented on the individual clients file, including why this decision was made. All data is kept, including special category data. Accounting records are kept for 7 years. These do not generally contain client data.
Dealing with new enquiries by email and telephone? (GDPR Principle 5 – storage limitation)	A sentence in the privacy policy for the website will state that all new enquiry data collected will be kept for a period of 12 months and then deleted. This covers those new enquiries that do not become official clients.
When and how is the data deleted? (GDPR Principle 5 – storage limitation)	After the appropriate retention period, all paper files are to be shredded using a professional secure shredding service. Digital files are deleted.

Retaining Personal Data (Storage Limitation) - Principle 5

Seen as a very contentious issue, this is the question of how long you should retain information on individuals. This has come to light in relation to insurance purposes for a private practice or case management company to professionally insure their business, as some insurance companies insist that personal data held on clients should be kept long term and not deleted.

Taken from the ICO website, the information provides reasoning as to how you should come to a decision in relation to retaining personal data on individuals.

The key point is that you must not keep identifiable data for longer than you need it and you must justify your reasons for keeping it as long as you choose to. If an individual requests you to delete their data you must review whether you still need to keep their data and act accordingly. Different rules apply to data kept for historical or scientific research purposes.

What should happen to personal data at the end of its retention period?

The General Data Protection Regulation does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

> Personal data kept in a form which permits identification of data subjects shall not be kept for longer than is necessary for the purpose for which it was/is processed.

This is the fifth data protection principle. In practice, it means that you will need to:

- 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; and
- update, archive or securely delete information if it goes out of date.

In some cases, you may need to keep personal data so you can defend possible future legal claims. However, you could still delete information that could not possibly be relevant to such a claim. Unless there is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise.

At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it. Automated systems can

flag records for review or delete information after a pre-determined period. This is particularly useful where many records of the same type are held.

However, there is a significant difference between permanently deleting a record and archiving it. If a record is archived or stored offline, this should reduce its availability and the risk of misuse or mistake. However, you should only archive a record (rather than delete it) if you still need to hold it.

You must be prepared to give subject access to it, and to comply with the data protection principles.

If it is appropriate to delete a record from a live system, it should also be deleted from any back-up of the information on that system.

The word ‘deletion’ can mean different things in relation to electronic data. The ICO has produced detailed guidance which sets out how organisations can ensure compliance with the DPA, in particular the fifth data protection principle, when archiving or deleting personal information:

For further information on this matter, please read:
https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

When can I refuse to comply with a request for erasure?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

The GDPR specifies two circumstances where the right to erasure will not apply to special category (health) data:

- If the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional);

- If the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices).

For further information on this matter, see here.

Mapping – Business Areas

Business area	Description of the work	Who is responsible for how this is carried out?
Invoicing	Invoicing clients or their representatives for work carried out. Use Paypal to produce invoices.	Isaac Oppey
DBS Checks	Only maintaining own personal DBS for clinician.	Susana Oppey
Client Record Management System	No specific system used at present. All client data is stored in documents and saved digitally or on paper.	Susana Oppey Isaac Oppey
T&C and Consent Forms	Generated as Word documents. Sent to clients as PDF via email, or as a hard copy. Hard copies are signed and then scanned. Video conference clients give consent verbally to the clinician.	Susana Oppey Isaac Oppey
Marketing activities	Emails to prior clients – not using a mailing list service right now, just a spreadsheet list. Website.	Susana Oppey Isaac Oppey

Technology used - what systems do you use for your processing activities?

Name of Technology	What the system is specifically used for	Who has access to the system
Simply Mail Solutions	Emails (hosting of emails) Email is also used as long-term storage/archive of client communication records.	Susana Oppey Isaac Oppey
Web Healer	Website (hosting of website).	Susana Oppey Isaac Oppey
Computer and Laptop	Accessing emails, the Internet, processing documents. Some client data is saved to the hard drive long term. Data from Dropbox is synced to hard drive.	Susana Oppey Isaac Oppey Both computers have password-controlled access. Only one login shared by both.
Mobile Phone	Client names and phone numbers are saved in phone memory.	Susana Oppey Isaac Oppey Phone has a passcode to access.
Dropbox	Cloud-based file storage and sharing platform. Some client data is saved here long term.	Susana Oppey Isaac Oppey
Paper-based records	Client data kept in hard copy is stored in a locked filing cabinet in home office.	Susana Oppey Isaac Oppey

Zoom, Microsoft Teams	Web based communication applications. Used to communicate with clients.	Susana Oppey Isaac Oppey
Paypal	Used for generating invoices to client's and receiving payments, therefore client data relevant to invoicing is stored within Paypal.	Susana Oppey Isaac Oppey

Information Notices – what are they?

The Information Notice as described below is a document to be sent out as an update to a client's current terms and conditions or as an update to an employee or associate's current contract/agreement.

Article 13 of the GDPR https://www.privacy-regulation.eu/en/13.htm identifies information which must appear within an information notice.

This includes:

- Name and contact details of the Data Controller;
- Contact details of the Data Protection Officer;
- Purpose and legal basis of the processing of information;
- Categories of personal data being processed;
- Details of any third parties the information will be shared with;
- How long the personal data will be kept;
- The data subject's right to request access to and amendments to be made or erasure of personal data;
- The data subject's right to restrict or object to the processing and the right to data portability *(data portability is the ability to move data among different application programs, computing environments or cloud services)*;
- The data subject's right to withdraw consent to processing at any time (if consent is relied on as a ground of processing);
- The right to lodge a complaint;
- Whether the data subject is under any legal requirement to provide the personal data; and
- Any automated decision-making or profiling and the consequences of this for the data subject (as an example, information collected on a subject that will help the organisation make decisions on what to send them automatically by email/newsletter etc.).

Where the controller has obtained/received personal data from a source other than directly from the subject themselves, additional information requirements apply. These further requirements are set out in Article 14 - https://www.privacy-regulation.eu/en/14.htm.

Limited exemptions from the information notice provisions will apply, for example where data subjects already have the information or where the provisions of the information are deemed impossible, would involve disproportionate effort or have obligations of professional secrecy.

Subject Access Request

New changes – be aware that Subject Access Requests are now free. You can no longer charge an administration fee, should a client/patient request details of the information you hold on them.

How does Pseudonymisation Protect Data?

Pseudonymisation is a novel concept in data protection, encouraged by the GDPR. It is a technique of processing personal data so that it can no longer be attributed to a specific individual without the use of additional information, which must be kept separately and be subject to technical and organizational measures to ensure non-attribution. Pseudonymous data, together with other security measures such as encryption, reduces the likelihood of identifying individuals, for example in case of a data breach or leak.

Pseudonymised information is still considered personal data, but the use of pseudonymisation is encouraged, since it is a technique which may satisfy requirements to implement “data protection by design and by default”; and it may contribute to meeting the GDPR’s data security obligations.

The application of pseudonymisation to e-health intends to preserve the patient's privacy and data confidentiality. It allows primary use of medical records by authorised health care providers and privacy preserving secondary use by researchers.

What about Anonymisation?

Anonymised data, i.e. that which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable, is not subject to GDPR regulations.

Anonymisation can therefore be a method of limiting your risk and a benefit to data subjects too. Anonymising data wherever possible is therefore encouraged.

Take care, however, as data must truly be anonymised for the GDPR not to apply. This means you must strip personal data of sufficient elements that mean the individual can no longer be identified. However, if you could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised.

Consent – are you up to date with this?

When does your business use consent? Example, consent forms when working with children and young adults.	A consent form is requested before carrying out the initial assessment, when meeting with the client for the first time. Consent is given for treatment (clinical consent, separate to GDPR) and also for certain uses of personal data where data usage does not meet the legal or contractual lawful bases (i.e. sharing data, audio recordings, marketing).
Are your current signed consent records valid, do they need updating?	Consent form to be updated to be GDPR compliant for future clients. Existing clients to be sent Information Notices.
How will you deal with records on your database that don't have consent in place?	Where consent is not given, we need to consider if we have other Lawful Bases under which to process the data, otherwise processing for which consent is not given/revoked must stop with that client until consent is reinstated.
Once the family/client has signed the consent form, how do you record this on your system?	Once signed, the consent form is kept as a hard copy in locked filing cabinets. Sometimes the consent form is scanned and saved digitally as well. Some clients only give verbal consent, which is recorded in their clinical notes.
How do you let people know they can withdraw from consent?	Information on the privacy policy on the reverse of the consent form informs them of their right to withdraw consent.

Data Protection Impact Assessments (DPIAs)

See this link for more information and guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. Most of the information on this page is taken from the www.ico.org.uk website.

A Data Protection Impact Assessment (DPIA) is a tool which can help businesses identify and minimise the data protection risks of a project. For any processing that is likely to result in a high risk to the individual, then you MUST carry out a DPIA. It is also good practice to do a DPIA for any major project involving personal data processing. DPIAs are often applied to new projects, because this allows greater scope for influencing how the project will be implemented.

Privacy risk is the risk of harm arising through an intrusion into privacy. This code is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those whom the person it is about does not want to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Projects which might require a DPIA:

- A new IT system for storing and accessing personal data; or
- A data sharing initiative where two or more organisations seek to link personal data.

An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. A DPIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

A DPIA must:

- Describe the nature, scope, context and purposes of the processing, including what data, recipients of data, and period of retention; a description of processing operations; list of assets on which data is processed (hardware, software, people, paper); and compliance with any codes of conduct is identified.
- Assess necessity, proportionality and compliance measures, including providing specific, explicit and legitimate purposes for processing, lawfulness of processing,

limited storage duration and what measures are in place to ensure data subjects rights can be exercised.
- Identify and assess risks to individuals, including noting origin, nature, particularity and severity of risks and the potential impact to data subjects' rights in the event of an incident; as well as identifying any additional measures taken to mitigate those risks; and
- Show that advice of the DPO/ICO and that the views of the data subjects or their representatives have been sought (where necessary).

Data Protection by Design & Default

Make sure any changes in your processing systems or operations always take into account what personal information you are using. Have you made everyone aware on your manual list of clients/customers that you are in the process of changing to a cloud-based system instead and how is their personal information going to be looked after?

Data protection by design is about considering data protection and privacy risks upfront in everything you do. The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This means you must factor data protection into your business activities right from the design stage of a new project, right through the lifecycle.

It can help you ensure that you comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

To understand this in more detail visit: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

In summary, the seven principles underlying Data Protection by Design are:
- Be proactive not reactive and preventative not remedial;
- Privacy should be the default setting;
- Data protection should form part of the core functions of systems/services;
- Full functionality – incorporate all objectives whilst also complying with obligations;
- End to end protection for data, for the full data lifecycle;
- Visibility and transparency to individuals, and systems premises and objectives and independently verifiable;
- Keep interests of users' paramount in design and implementation.

Appointment of a Data Protection Officer

When does a Data Protection Officer need to be appointed under the GDPR?

If your organisation is a public body, or your core business activities involve large scale processing of Special Category data (health being one of them) or systematic monitoring of individuals, then it is mandatory to appoint a Data Protection Officer.

There is no specific detail on size of business, though it is anticipated that sole traders and companies having 5 or fewer staff members will not be required to have a DPO in place.

Information on this page and the next taken from:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

What are the tasks of the DPO?

The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and
- To be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc).

What does the GDPR say about employer duties?

You must ensure that:

- The DPO reports to the highest management level of your organisation, e.g. Director;
- If the DPO is an internal member of staff within your business, the DPO operates independently and is not dismissed or penalised for performing their task; and
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

Can we allocate the role of DPO to an existing employee?

- Yes. If the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests.
- You can also contract out the role of DPO externally.

Appointment of a Data Protection Officer continued…

Does the data protection officer need specific qualifications?

- The GDPR does not specify the precise credentials a data protection officer is expected to have.
- It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

Do we have to publish details of the DPO?

Yes, the GDPR requires that you publish the details of your DPO and inform the ICO of who the DPO is. Remember that if you don't have to appoint a DPO but you decide to do so voluntarily you will still need to meet the same duties and responsibilities regarding the DPO as if it was a requirement.

Having these good practices in place, as below, should rule out any unnecessary reviews:

- Having a good overview of the business;
- Good risk assessments in place;
- Well trained staff; and
- Name of the DPO made available on all external policies.

Breach Notification

Information on the next 7 pages has been taken from these links on the ICO website:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

https://ico.org.uk/for-organisations/gdpr-resources/pdb/

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

The GDPR places a duty on Data Controllers to report serious breaches to the attention of the Information Commissioner's Office. 'Serious breaches' are not defined, but it your responsibility to risk assess and establish the likelihood and severity of harm to an individual's rights and freedoms as a result of the breach. If harm is likely, you must report it; if harm is unlikely you don't have to, but you should document your justification for making this decision.

Reading further information from the link above should assist Data Controllers in considering whether breaches should be reported.

Where there is uncertainty, contact the ICO for assistance so that the nature of the breach or loss can be considered, together with whether the data controller, to ensure the business is properly meeting its responsibilities under the DPA.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. It is difficult to be precise about what constitutes a large volume of personal data. Every case must be considered on its own merits.

Breach Notification continued…

Here are some examples of breaches, showing which ones should be reported to the ICO:

Reportable Breach	Not Reportable Breach
Theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of 100 individuals.	Theft or loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the product being marketed.
A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to 50 named individuals and their financial records.	A similar system holding the trade union subscription records of the same number of individuals, where there are no special circumstances surrounding the loss.

Further Examples

The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.
Your organisation (the controller) contracts an IT services firm (the processor) to archive and store customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies you that the breach has taken place. You in turn notify the ICO.

Breach Notification continued…

Further Examples

You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system. You notify the ICO within 72 hours of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the ICO more information about the breach without delay.
A hospital suffers a breach that results in an accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.
A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals. They don't need to be informed about the breach.

Failing to notify a breach when required to do so can result in a significant fine of up to 10 million euros or 2 per cent of your global turnover. The fine can be combined with the ICO's other corrective powers under Article 58. It is important to make sure you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time; and to provide the necessary details.

Breach Notification continued…

Conditions where notification is not required

Article 33 of the GDPR makes it clear that breaches that are "unlikely to result in a risk to the rights and freedoms of an individual" do not require notification to the ICO.

An example might be where personal data is already publicly available and a disclosure of such data does not constitute a likely risk to the individual.

Further conditions where communication is not required:

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption.

- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individual(s) is no longer likely to happen. For example, the 0.controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it.

- It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner.

Further information on this area can be seen at this direct PDF link.

Breach Notification continued…

What information must a breach notification contain?

- The nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- The name and contact details of the Data Protection Officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Notifying a Breach and Time Period

The Data Protection Officer has a period of 72 hours to report a breach to the ICO, from the time the actual breach took place.

As an example, if a data breach took place at 4.30pm on Friday afternoon and this was left until Monday morning to report to the DPO, the DPO would only have a small window available, until 4.30pm Monday to report the breach to the ICO.

Method of reporting

Serious breaches should be reported to the ICO using their DPA security breach helpline on 0303 123 1113 or 01625 545745 (open Monday to Friday, 9am to 5pm), or using the functionality contained within the DSP Toolkit (https://www.dsptoolkit.nhs.uk/).

Attached with this document is the **Data Protection Breach Notification Form**.

This gives you full details of how to fill in the form, how to send it back and what happens next.

Chain of command and how to prepare for breach reporting?

- Your staff/team should understand what constitutes a data breach.
- Risk assessments have been carried out.
- An internal breach reporting procedure is in place and all staff are aware of this.

This reporting procedure will help facilitate decision-making about whether notification to the ICO is necessary.

Breach Notification continued…

Accountability and Record Keeping

Regardless of whether or not a breach needs to be notified to the ICO, the controller must keep documentation of all breaches. Having a Data Protection Breach Register in place is a good idea.

Taken from this direct PDF link, the ICO says:

> "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

Whilst it is up to the controller to determine what method and structure to use when documenting a breach, in terms of recordable information there are key elements that should be included in all cases.

In addition to these details, it is recommended that the controller document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented.

This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals. Alternatively, if the controller considers that any of the conditions are met, then it should be able to provide appropriate evidence that this is the case.

Where the controller does notify a breach to the ICO, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.

Where the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.

It should be noted that failure to properly document a breach can lead to the ICO exercising its powers under Article 58 and or imposing an administrative fine in accordance with Article 83.

Breach Notification continued…

How long should you keep these records for?

The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data and to meet a lawful basis for processing.

It will need to retain documentation in so far as it may be called to provide evidence of compliance, or with the accountability principle more generally, to the ICO. Clearly, if the records themselves contain no personal data then the storage limitation principle of the GDPR does not apply.

Fines

When the GDPR is enforced from 25 May 2018, breached organisations will find the fines they face increasing.

It clearly states on the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/?q=fine:

"Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover."

Who has responsibility?

It is important that all staff/team members are well trained and are aware of what constitutes a data breach, to help ensure the organisation is able to meet its obligations.

Where a Data Processor is used, they are responsible for notifying the Data Controller in the event of a breach. The Data Controller is then responsible for notifying the ICO. Breach reporting requirements should be detailed in the contract between the Controller and Processor.

A processor may be contractually liable to the controller for any failure to meet the terms of their agreed contract. It will also be subject to investigation by the ICO and may be subject to administrative fines or other penalties.

If a processor acts outside of a controller's instructions in such a way that it decides the purpose and means of processing, then it will be a controller and will have the same liability as a controller.

Penalties for not registering with the ICO

You are breaking the law if, as a controller, you process personal data, or are responsible for the processing of personal data, for any of the non-exempt purposes and you have either:

- not paid a fee, or
- not paid the correct fee.

The maximum penalty is a £4,350 fine (150% of the top tier fee.)

Marketing Policy

Specific rules apply under the Privacy and Electronic Communications Regulations (PECR), if you are asking people to consent to receive direct marketing.

If you want individuals to consent to direct marketing, you should have a separate, unticked, opt-in box for this, prominently displayed.

Consent may not be needed to undertake direct marketing by post or phone call (unless the individual is registered with the Telephone Preference Service), if another processing condition can be relied on. But the ICO considers gaining consent to do this to be good practice and the most advisable approach.

If you wish to email an individual you have not made contact with before and do not have their consent, you will need to gain consent by other means instead.

For example:

- Meet them at a conference or networking event you know they will be attending and ask if you can send them an email.
- Make contact with them via LinkedIn, sending them an initial invite message.
- Send them a letter explaining what your service/product is about but must remember to include a 'privacy notice' that specifically asks for their consent.

For further information see - https://ico.org.uk/for-organisations/marketing/

Answers to those General Questions on Marketing – GDPR style

Here is a selection of questions (scenarios) in relation to the GDPR. What are your thoughts on this? Are you aware of the new changes in relation to marketing by email, posting out and making phone calls? Will it affect your business?

QUESTION
Currently we have over a thousand people on our database. Will we need to send them all an information notice telling them we are complying with GDPR, giving them the option to unsubscribe, telling them how their information is being used, and giving them the option to be removed from our database?

ANSWER
You need to ask yourself how you got hold of their contact details (email addresses) in the first place. Did you find them on their website or from an industry directory online and copy and paste the information into your database?
If so, you will need to make them aware of how you came across their details, giving them the option to unsubscribe and be removed from your database.

QUESTION
What does 'Implied Consent' mean?

ANSWER
Implied Consent means consent which is not expressly granted by a person, but rather implicitly granted by a person's actions or by a person's silence or inaction.

You could suggest that, if a person willingly puts their contact details on an industry database, which then sits on a website for anyone to see or search for, that it would be acceptable to take their contact details and add them to your own business database for marketing purposes. It's already out there, for public consumption.

But the GDPR is now asking that consent must be properly specified. You must seek acceptance from individuals allowing you to hold their details on your database. You can't just presume.

QUESTION
If we attend a conference and are given a delegate sheet of attendees, what's the best way of using this information to make contact with people?

ANSWER
A good option is to find the people on LinkedIn and ask to connect with them.
Mention you attended the XYZ conference in X-Town, didn't get the opportunity to chat with them and hoped they would be happy to connect with you on LinkedIn.
Once they connect with you, then you can ask them further questions, including asking for permission to add them to your database to receive your monthly newsletter.

QUESTION
What are the Mail Preference Service and the Telephone Preference Service?

ANSWER
Under the Privacy Regulations it is a legal requirement to check your database regularly with the Telephone Preference Service (TPS) to ensure that the people (businesses and individuals) you are calling are not registered.
Similarly, with the Mail Preference Service (MPS), although it is not a legal requirement, screening against the MPS is required under the CAP Code and the DMA Code.

QUESTION
Can you explain more about 'Opt-out' requests?

ANSWER
- Whenever you contact a potential customer, make sure you provide a clear statement of the marketing company's identity and contact details.
- Individuals can opt out of marketing contact at any time. The only cost to the customer of opting out should be the cost of sending the message; they must not incur a premium rate charge. It is important to record such requests accurately and to act on them promptly.
- It is important to include an opt-out opportunity on all pieces of direct marketing, whether sent by mail, e-mail or SMS.
- Opting in or out of marketing contact should be made as simple as possible for the individual, for example by providing a link to unsubscribe in an e-mail or allowing individuals to text STOP to a given number.
- If someone opts out of marketing, ensure that you retain their record on the system and note that they have opted out (known as "suppressing" the details). If you simply delete their details, you may obtain their data later from another source and will not know that they have opted out of marketing contact.
- It is not acceptable to rely on silence as an opt-in. You need some positive action by the customer, such as returning a form or an e-mail.

Practical ways in dealing with new enquiries on the phone and selling services, while being GDPR compliant

QUESTION

We often have telephone enquiries where we will take details which end up on a database.
We will use the details for handling the enquiry, but we may also get in touch with the person if for example we have a significant reduction on a product or service they might be interested in.
My question is, how do we prove consent when somebody has offered their details over the phone?

ANSWER

Explain that their personal data will be destroyed once the transaction is completed. Unless there is a warranty period, and the customer has to be known during that period. In any case, the customer should be notified about how long their data will be with you.

Use a statement such as "We'll keep your contact details until you tell us to remove them, but for no longer than a year after you last spoke to us."

If the process involves getting an email address, then a simple privacy notice can be sent, but telephone conversations need to be simple, for the sanity of all concerned.

Practical commonsense approach is all that's needed. No need to over engineer.

If you're clear with your customers about:

- what information you have;
- why you're using it;
- act on their instructions to stop using and delete as required;
- along with documenting your rationale for your practical approach,

this will show that you've given thought to the privacy rights of your customers and your approach to data protection compliance.

Working in the Cloud

The GDPR allows Cloud Service Providers (CSP) processors to demonstrate compliance with many of its requirements (including the security and general processor obligations) by either:

- adopting approved 'Codes of Conduct' and/or
- participating in certification or seal programmes that are approved by Supervisory Authorities (e.g. possibly the TRUSTe enterprise privacy certification or, in the UK, a Privacy Seal).

These compliance steps will also be useful to controllers evaluating and assessing processing services as a part of their mandated data protection impact assessments.

Certification types

The Certified Mark identifies an organisation that has Self Certified to the Cloud Service Provider Code of Practice and the public declarations are accessible on the supplier's website and the Cloud Industry Forum (CIF) website Register of Certified Organisations.

The Certified+ Mark is a higher-level mark that identifies an organisation that has been independently assessed by an Accredited Assessor as being compliant with the Code of Practice. The public declarations will be visible on both the supplier's own website and the CIF website register of certified organisations.

Information below and on the next page is taken from the cloud storage provider www.tresorit.com

What are the advantages of using end-to-end encrypted cloud services?

If a data controller uses an end-to-end encrypted service as processor, the related personal data 'stays within their company walls'. Therefore, end-to-end encryption has substantial advantages that help controllers better protect data, making compliance process easier and cost reducing.

The data controller will result in compliance with Article 32 GDPR.

Secondly, if a strong encryption mechanism is implemented and the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, the data controller will likely be exempted from notifying the data breach to the supervisory authority and communicating it to the affected data subjects pursuant to Articles 33 and 34 GDPR.

Working in the Cloud continued…

Moreover, except the duties of assistance to the controller pursuant to Article 28 GDPR, the processor will likely fall out of the audit scope in case the controller is audited, making compliance and audit process simpler for the controller.

How does encryption help with protecting data and compliance?

Encryption is underlined as an example of “appropriate technical and organisational measures” and an appropriate safeguard to protect data.

The GDPR states that if the controller has implemented encryption to its personal data, in case of personal data breach, affected personal data are likely be unintelligible to any person who is not authorised to access it. Hence, such data breach is unlikely to result in a risk to the rights and freedoms of affected natural persons.

The result is that the controller may not be required to communicate the data breach to affected data subjects, pursuant to Article 34 GDPR.

All in all, encryption reduces the risks of processing data in the cloud, as it reasonably makes reidentification of leaked personal data impossible with reasonable measures. The more the encryption algorithm is strong, the more it may reduce the liability of data controllers.

What is the difference between encrypted data and anonymous data?

While encryption is one of the “appropriate technical and organizational measures” to protect data according to Article 32 GDPR, anonymous data is any data that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

In other words, encryption relates to security of personal data whilst anonymization refers to permanent de-identification. The GDPR applies to encrypted data but it does not apply to anonymised data.

Cloud Services – GDPR Compliant Companies

It is also recommended to visit the Privacy Shield website

Here is a typical list of companies showing their GDPR compliancy.

Company	Listed on Privacy Shield	Has a security certificate or information on their website
www.writeupp.com (Practice management system)		Yes
www.qunote.com (case management system)		Yes
www.iinsight.biz/ (Case management system)		Yes http://www.iinsight.biz/files/ISO27001-2013-certificate.pdf
Microsoft SharePoint	Yes	Yes https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx
Dropbox (business version)	Yes	Yes https://www.dropbox.com/help/security/general-data-protection-regulation
Google docs	Yes	Yes https://www.blog.google/topics/google-cloud/google-cloud-our-commitment-general-data-protection-regulation-gdpr/
Tresorit (cloud storage service)		Yes https://tresorit.com/gdpr
Mailchimp (Newsletter marketing)	Yes	Yes https://mailchimp.com/gdpr/
Hubspot (CRM platform)	Yes	Yes https://www.hubspot.com/data-privacy/gdpr
Skype (Microsoft)	Yes	Yes

Company	Listed on Privacy Shield	Has a security certificate or information on their website
LogMeIn GoToMeeting (conference calls)	Yes	Yes https://blog.gotomeeting.com/goto-products-gdpr/
IdleServ (domain/web hosting)		Yes https://idleserv.net/privacy-policy
RackSpace (cloud storage service)	Yes	https://www.rackspace.com/en-gb/gdpr
GoDaddy (email/website hosting)	Yes	https://uk.godaddy.com/help/what-does-gdpr-mean-for-my-business-27935
Microsoft 365		Yes https://blogs.office.com/en-us/2018/02/22/microsoft-365-provides-an-information-protection-strategy-to-help-with-the-gdpr/
PracticePal (Practice management system)		Yes http://www.practicepal.co.uk/gdpr/
Google Cloud		Yes https://cloud.google.com/security/gdpr/