Northern Independent Mediation

Data Protection Policy (GDPR)

August 2018 Version 1.1

Contents

GDPR (General Data Protection Regulation) will become UK law on **25 May 2018.**

If you use information about other people to do your job, this new legislation will affect you.

This guide highlights the main things NIM staff need to **know** and **do** to make sure we comply with GDPR.

Protecting data is everyone's responsibility

- What do we mean by personal data, or personal information?
- Do you know what personal information you hold and where?
- Would your customers, clients or contacts be surprised to know how you use their data?

Personal information means any information about a living person – staff, service users, citizens or anyone else – when you can see or work out who that person is.

As well as personal details (name etc), it can include correspondence, photos, audio recordings and video recordings.

GDPR replaces the Data Protection Act and is more rigorous in its rules.

When we get information from people, we must be clear and specific about how we are going to use it, and why.

Everyone is responsible for ensuring the data we collect and use is handled and stored properly, and used in the correct, lawful way.

The basics

You must look after the information about people that has been entrusted to you.

If you handle people's personal information in your job, you must comply with the GDPR rules.

If in doubt, speak to the Managing Director, Registered Manager or Senior Mentor.

Complying with GDPR

- We must have genuine, fair and lawful reasons for collecting and using people's personal information.
- We must be open and clear about how we will use people's information.
- We are only allowed to collect the information we need.
- We must handle information about people only in the ways we said when we collected it.
- We must make sure the information we use is accurate and we should not keep it for longer than it is needed.
- GDPR does not apply to records about people who have passed away, although this data could still be protected by other legal rules.

Privacy notice

- We use a form called a **privacy notice** to explain to people how and why we use their information.
- Some information collection is permitted under rules including 'public task', 'public interest', 'performance of a contract', 'vital interests of a data subject' and other categories.
- Most services will need to obtain people's **consent** to use their information – this is explained in a separate section.
- You should be familiar with the privacy notice for your service area. It is **your responsibility** to play your part in complying with what it sets out.

Your service, your responsibility

Protecting information is everyone's responsibility. What do services need to consider in particular?

Privacy notice

This document makes it clear to the public what we will use their information for and why.

It is your responsibility to understand your service's and Northern Independent Mediations privacy notices and comply with the assurances we have provided to people.

Data sharing agreements

If we are sharing information with other organisations, we use a data sharing agreement.

It is your responsibility to share information appropriately, only providing what is needed and what you are permitted to share.

Information asset registers

Northern Independent Mediation must keep a record of all the systems or databases that you use, which store or process people's personal information.

This may include online data management systems, our drives (Physical or Cloud based) or even paper files.

All these systems and stores must have appropriate security to protect people's information.

It is your responsibility to use these systems correctly and ensure systems you use are included on your information asset register.

Lawful basis for processing information

There are a number of 'lawful' reasons which allow NIM to use, process and store people's personal information.

The reasons include:

- Performing a task in relation to the business
- Protecting someone's 'vital interests', including on behalf of someone who is not able to give consent themselves
- Carrying out obligations under employment law
- Performing a task in the public interest
- Activity relating to legal claims
- Working to deliver a contract

There are other reasons, including when someone has provided **consent** for their information to be used.

Your service's **privacy notice** will explain the lawful basis why your service uses personal information.

Gaining people's consent to use their information

Some NIM services, such as marketing and communications, use gaining people's **consent** as the basis for collecting and using their personal information.

When using consent as the legal basis, there are a few important things to consider.

- Use 'consent' as the legal basis if no other reason can apply.
- People must actively 'opt in' – pre-ticked boxes are not allowed.
- We can only collect information for a specific purpose – not 'just in case' we need it.
- We must be clear why we are collecting the data and everything must be explained in plain English.
- People have the right to withdraw consent and we must make this clear in our communications.
- There must be an effective way for people to withdraw consent and we must have a process in place to remove people's information from databases when requested.
- We must keep good records of the information flow including how the consent was obtained.

People's rights

People have increased rights under GDPR. We must respect this and take action to address any issues

1. The right to be informed.
We are clear with people how we will use their information – how it is collected, stored, handled and protected. We explain this to people in a privacy notice.

2. The right of access.
People can request to see all the information we hold about them under a 'Subject Access Request' (SAR). The request must be made in writing and we must respond within one month.

3. The right to correction.
We must correct any wrong or incomplete information within a month of being asked. We must also ask third parties to also amend their systems accordingly, if we have provided them with the information.

4. The right to be forgotten.
If information was collected under people's consent, or if the need for the information has expired, people can ask for their information to be erased. We must respond to a request within one month. We do not have to remove the data if we need it for a legal reason.

5. The right to restrict processing.
If someone tells us we may have the wrong information about them, we must stop processing their information while we make checks. The investigation and any corrections must be done within one month.

6. The right to data portability.
This allows people to obtain and reuse their personal data for their own purposes. It particularly applies to consumer services, such as banking, where people might want to look for a better deal.

7. The right to object.
People can complain, if they feel we should not be using their personal details or information about them. If we are using their details for marketing purposes, we must stop immediately. In other situations, we must first check whether there is a legitimate reason for using the information, over and above the individual's wishes.

8. Automated decision-making including profiling.
This applies to using people's information for profiling purposes or for decisions taken by automated processes. This is restricted and in general we must obtain people's consent. There is a detailed checklist on the ICO website.

Subject Access Requests (SARs)

A Subject Access Request is when a person asks to see a copy of the information we hold about them.

People have the right to ask for this.

If someone makes a verbal request, you must ask them to put this in writing.

The request can be made in any written format – even social media.

Under GDPR we must respond to SARs without delay and within **one month.**

Occasionally this can be extended for complex requests.

How much time should we spend on responding?

If you receive a SAR, you must take **reasonable steps** to respond.

Sometimes a request may be straightforward, but sometimes there might be challenges with obtaining all the information, if it is held across different servers, systems and archives.

If possible you should discuss the request with the individual to understand what information they want, so you can be more specific in your response.

You can refuse to respond to a request if it is excessive, repetitive or 'unfounded' (such as if we do not hold the data they think we do).

If you refuse to respond to a request, you must explain **why** to the individual, informing them of their right to complain. You must do this within one month.

When things go wrong - confidential information breach

An information breach is when confidential information **is lost, stolen, incorrectly used**, or **shared with the wrong person or people**.

Sometimes breaches are deliberate, through theft or malicious attack. But many information breaches happen through lack of awareness or by accident.

We do everything we can to avoid mistakes and attacks, but if there is an information breach, there are important steps you must take, as quickly as possible.

With GDPR, the rules for reporting breaches are stricter than before, and the penalties can be more severe – up to £20 million fines for large organisations.

A breach could be…

- Lost laptop or written notes
- Emailing or posting personal information to the wrong person
- Losing or deleting information so it is no longer available
- Altering information without permission
- Opening a malicious virus email
- Using personal information incorrectly

Information breach – what to do

If you discover or cause a breach, tell the Managing Director, Registered Manager or Senior Mentor straight away

All breaches which could cause significant harm to individuals must be reported to the Information Commissioner's Office (ICO) within 72 hours.

Potential harm includes discrimination, damaged reputation, financial loss, loss of confidentiality or any other economic or social disadvantage.

In some cases, we must inform the people affected by the breach, depending on the level of risk or harm to them.

Sharing information

Looking after people's information doesn't mean we can't share it at all.

We can share information with other departments or organisations in some circumstances. For example:

- If we have a sharing agreement
- In an emergency
- If you can justify the benefits to the individual outweigh the risks

How your service shares people's information is explained in your service's privacy notice.

Taking photos

Sometimes NIM wishes to store and use photos (or videos) of people, such as for reports or marketing.

Images are classed as data. Where individuals can be clearly recognised from the image, this is generally bound by the 'consent' legal basis, so permissions must be obtained and correctly documented.

For more information, including example consent forms, please contact the office.

Special category data

This is information that is considered to be especially private or sensitive, and so needs more protection.

Special category data, sometimes known as 'sensitive personal data' has been updated for GDPR.

There are new categories included. We need to consider the lawful basis for processing this special information, in the same way we do for other types of personal information.

The special categories are:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sex life
- Sexual orientation

Storing information

People's personal information must be stored in a secure place

- Use the correct secure, central system.
- If there isn't a system, keep it in a password-protected area.
- Don't keep duplicate copies that could become out of date.
- Be aware of how long information can be kept and delete or destroy it when appropriate.

How long should I keep information?

Some services have statutory 'retention periods' – the amount of time we must keep information in case someone requests it or we need to refer to it.

If there is no statutory retention period it is up to the service to decide how long to keep information, including people's personal information.

Information should only be kept for as long as it is needed, then it should be destroyed.

Bear in mind people's rights – the longer people's information is kept for, the more complicated it may become to answer subject access requests etc.

Looking after colleague information

Do you need to keep any personal information about staff in files such as Word or Excel? For example: return-to-work interviews, sickness data or disciplinary information?

Personal information about staff and/or details provided to you privately by colleagues must be stored confidentially.

Store any information that does not belong in a specific system in a password protected area, our CRM Database, or SharePoint, when available.

Don't keep information you don't need – delete or shred it. Commercial shredders are available at both of our offices for use by all staff.

Working with suppliers

When we hand over other people's personal information to suppliers or contractors, in order for them to perform a task for us, they become a **data processor.**

We are responsible for making sure our data processors handle information correctly and comply with GDPR.

A few examples

There are lots of ways we use other companies or organisations as data processors. Examples could range from providing services to vulnerable people, to services that involve staff transfers.

Even digital systems or 'software solutions' from a third party to help NIM staff do their work would need to be considered and the contracts revised.

Updating the wording in our contracts

We are in the process of updating the wording in our contracts to spell out what we require of our suppliers and partners under GDPR. Contracts must:

- Explain what personal information is being used or processed.
- Provide instructions for exactly how the data is to be used.
- Set out the standards expected of the supplier, including the security of their own systems and how they must correctly handle the data we provide.
- Set out how we require suppliers to delete or return data at the close of the contract.
- Explain the suppliers' role in supporting subject access requests or other responses to people's rights under GDPR.
- Explain the suppliers' duty to report any data breaches.
- Identify how we will audit or monitor the correct use of data we provide.

GDPR – more information

Find out more about visit the ICO website: **https://ico.org.uk/**

How we manage our records

Our Server & Database

All records and information is held on our secure database 'lamplight'. This is hosted on the Amazon Web Services server which is certified to ISO270001 in addition to numerous others.

No client data is permanently stored on any device or in house server to ensure the confidentiality of all data, due to the very nature of our service our policies in regards to data control exceed that required by the GDPR regulations.

At NIM we do not keep any physical records for more than 24 hours other than where entirely unavoidable due to external requirements such as specific client need.

Encryption of NIM devices.

We recognise that certain data will unavoidably be held in the short term on devices such as laptops and mobile phones, this for example will include emails, contact details etc. Prior to there entering onto our secure server.

As such all such devices are encrypted to ensure that in the unfortunate event that such a device falls outside of our immediate control such as by theft; that any such data held is irretrievable by any third party.

Devices used by NIM and how they are encrypted are as follows;

Device Type	Type of Data Held	Encryption Method
Laptops	Emails Client Data prior to upload	All machines used are windows based and encrypted using Bitlocker, this provides full encryption of all data stored preventing its retrieval including by the use of data recovery techniques.
Desktop PC's	Emails Client Data prior to upload	As per laptop PC's.
Mobile Phones	Emails	All mobile phones used by NIM, are manufactured by apple and benefit from apples own data encryption. In addition they are set so that all data is wiped where a party attempts to enter the
Tablet's	Emails	As per for Mobile Phones
USB Drives	Not Used By NIM	N/A
CD/DVD	Not Used By NIM	N/A
Memory Cards	Not Used By NIM	N/A

Security of physical copies of data.

It is NIM's policy that no hard copies of any documents should be kept unless strictly required, and that they are to be immediately securely disposed of upon their uploading to our secure service.

In order to prevent any breach of data, all documents are to be kept in a secured file cabinet which must be kept locked. When the documents have been uploaded to the secure server, the documents must be shredded with a shredder rated to DIN66399 level 5, such services are available at our office in Bradford.

How we Process Data

The data potentially processed by NIM is handled according to the nature of that information, the following provides an overview of how that data is processed.

Data Type	How Stored	Reason for Processing	Accessible by	Length Retained	How handled at expiry
Client Name	Secure Server	Case specific management Identification of Records Contact with Parties	Mediation Clerks Assigned Mediator	6 years or project length	Permanently deleted
Client DOB	Secure Server	Case specific management Identification of Records Contact with Parties	Mediation Clerks Assigned Mediator	6 years or project length	Permanently deleted
Client Address	Secure Server	Case specific management Identification of Records Contact with Parties	Mediation Clerks Assigned Mediator	6 years or project length	Permanently deleted
Client Contacts	Secure Server	Contact with Parties	Mediation Clerks Assigned Mediator	6 years or project length	Permanently deleted
Referring Organisation	Secure Server	Case specific management Identification of Records Contact with Parties	Mediation Clerks Assigned Mediator	6 years or project length	Permanently deleted
Case Specific Documents	Secure Server	Case specific management	Assigned Mediator	Case duration (avg 28days)	Permanently deleted
Work Records	Secure Server	Case specific management	Assigned Mediator	Case duration (avg 28days)	Permanently deleted
Mediation Contracts	Secure Server	Case Specific management Business requirements Availability to clients and clients representatives	Mediation Clerks Assigned Mediator	6 years	Securely Archived accessible only to nominated system administrator by request.
Mediation Agreements	Secure Server	Case Specific management Availability to clients and clients representatives	Mediation Clerks Assigned Mediator	6 years	Securely Archived accessible only to nominated system administrator by request.
Referral Information	Secure Server	Case specific management	Mediation Clerks Assigned Mediator	6 years or Project Length	Permanently deleted
Outcome Statistics	Anonymised	Performance monitoring Requirements of Contract Regulatory Body Requirements Staff Development Staff professional requirements Business marketing purposes	Public	Indefinite	N/A
Evaluation Statistics	Anonymised	Performance monitoring Requirements of Contract Regulatory Body Requirements Staff Development Staff professional requirements Business marketing purposes	Public	Indefinite	N/A
Case Type Statistics	Anonymised	Performance monitoring Requirements of Contract Regulatory Body Requirements Staff Development Staff professional requirements Business marketing purposes	Public	Indefinite	N/A
Referral Outcomes	Secure Server	Requirements of Contract	Mediation Clerks	Project Length	Permanently deleted
Case Studies	Anonymised	Performance monitoring Requirements of Contract Regulatory Body Requirements Staff Development Staff professional requirements Business marketing purposes Training & Development	Public	Indefinite	N/A