Forum Data Protection Policy

Incorporating the EU General Data Protection Regulations (GDPR)

March 2018

Introduction

This policy has been drawn up to ensure that the organisation and its employees, volunteers and partners comply with the Act. Everyone is individually responsible for compliance with the Act and ensuring that they do not breach any part of it.

This policy must be read in conjunction with the IT security, e-mail and Information Governance policies and all staff must sign a statement to show that they have read, understood and will abide by the policies (Appendix d)

The Regulation

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

What information does the GDPR apply to?

Personal data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data" (Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. These must be processed in accordance with Article 6

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (Article 10).

Definitions

- A Data Controller determines the purposes and means of processing personal data. For the purposes of this Policy, the North Bank Forum is the Data Controller

- A Data Processor is responsible for processing personal data on behalf of a controller. For the purposes of this policy, a processor is a project that collates and manages personal data on behalf of NBF. Payroll and Pension companies are also classed as Data Processors

- Data Protection Officer. The regulation requires that they have “expert knowledge of data protection law and practices.” And that the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests. Under the GDPR, you must appoint a DPO only if you:
    - are a public authority (except for courts acting in their judicial capacity);
    - carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
    - carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

  None of these apply to the rest of our business. However, should a serious issue arise, we would have to approach an external body or individual to act as out DPO

- Data Privacy Officer. This is the individual nominated to ensure that the organisation fulfils its duties under GDPR, but is not a Data Protection officer. For the purposes of this policy, the Data Privacy Officer is Ali Middle

The Principles

Under GDPR Article 5 there are 6 principles requiring that personal data must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals; The lawful bases for processing are set out in Article 5 of the GDPR. At least one of the following 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.)

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

    a) You must not collect information unless there is a specific and valid reason
    b) Must not be used for any other unrelated purpose

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

    a) Only data needed for the specific purpose should be asked for or recorded.
    b) Information that is not relevant must not be collected simply because it might be useful in the future!

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

    a) Data users should record information accurately and reasonable steps should be taken to check accuracy
    b) All data storage systems should be “spring cleaned” to destroy inaccurate and out of date information

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.

    a) It is already the case that controllers must inform subjects of the period of time (or reasons why) data will be retained on collection.
    b) Should the data subject subsequently wish to have their data removed and the data is no longer required for the reasons for which it was collected then it must be erased.

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The rights of the Data Subject

The GDPR provides the following rights for individuals:

a) The right to be informed
   - Individuals have the right to access their personal data and supplementary information.
   - The right of access allows individuals to be aware of and verify the lawfulness of the processing.

b) The right of access - under the GDPR, individuals will have the right to obtain:
   - confirmation that their data is being processed;
   - access to their personal data; and
   - other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

c) The right to rectification
   - Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
   - If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

d) The right to erasure
   - Individuals have a right to have personal data erased and to prevent processing in specific circumstances:
   - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
   - When the individual withdraws consent.
   - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
   - The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
   - The personal data has to be erased in order to comply with a legal obligation.
   - The personal data is processed in relation to the offer of information society services to a child

   However, there are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.
-

e) The right to restrict processing
   - individuals have a right to 'block' or suppress processing of personal data.
   - When processing is restricted, you are permitted to store the personal data, but not further process it.
   - You can retain just enough information about the individual to ensure that the restriction is respected in future.

f) The right to data portability
   - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
   - It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

   The right to data portability only applies:
   - to personal data an individual has provided to a controller;
   - where the processing is based on the individual's consent or for the performance of a contract; and
   - when processing is carried out by automated means.

g) The right to object - Individuals have the right to object to:
   - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
   - direct marketing (including profiling); and
   - processing for purposes of scientific/historical research and statistics.

h) Rights in relation to automated decision making and profiling
   The GDPR has provisions on:
   - automated individual decision-making (making a decision solely by automated means without any human involvement);and
   - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Staff Responsibilities

Data collection and processing

Active compliance from the data subject must be obtained for the collection of any personal data. Personal data is anything that can identify individuals elsewhere. Examples include name and address, anything to do with medical matters, employment history,

The data subject must be informed as to what information is being collected, the legal basis for collection the information (See Principle 1), and the specific purposes.

Separate consent must be obtained for **each** purpose. .All forms should include a release as a matter of course, and this should be signed to indicate active consent. A sample Data Protection Release is attached at the end of this document as appendix (a) for guidance

If taking verbal information or a referral, inform the other person that you will be recording the information they provide in accordance with Article 6(a) and ask them if they consent to doing so. Preferably, request that they go online to provide their details or in writing.

If information is being passed on you must ensure that we have permission to do so from the individual. No personal information must be passed on without this consent

If information is being passed to us, e.g. from Social Services, ask whether the client is aware that they are doing so. It is not our responsibility to inform the client that we now have the information and record the answer, but it is our responsibility to ascertain the facts.

Only authorised people can see personal information, including staff records.

Security

All hard copy personal data must be kept in locked cabinets etc. This will include all personnel files.

We must aim to operate a clear desk policy. This means that no personal information must be left on your desk when you are not there. This includes short breaks.

Computer screens must be sited to ensure that unauthorised people cannot see personal information, e.g. away from windows, where at all possible. Screens must be locked if you are leaving your desk for any length of time

If taking personal information out of your office as hard copy, place it in a sealed envelope and log what has been removed from the building.

Data held in electronic format must be secured either by password or encryption

Passwords or PIN numbers must be changed periodically where necessary.

Ensure that any personal information deliberately deleted from your computer (and where you envisage never needing it again) is irrecoverable.

Name computer files with a clear, meaningful title to avoid confusion and accidental deletion.

Dispose of paper personnel files securely, e.g. shredded.

Take reasonable precautions to protect computers and manual files from theft and physical damage, e.g. leave laptops in the locked boot of your car when out, do not leave it on view to the public at home or next to a ground floor open window in the office etc. Use common sense precautions.

When sending information via email do not include any personal data other than basic details such as name and address. Do not send any sensitive information. Emails are not secure.

Incoming email containing personal data must be deleted within one working week unless the personal data contained is needed for a specific purpose and the sender is aware of that purpose.

Client information must be kept up to date and only held for 2 years after our last contact with them unless specified otherwise. (See pages 10 and 11 for guidance)

Data breaches

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 includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it and report it to the Data Privacy Officer.

Recruitment

All application forms must include a data protection consent, and the Recruitment Privacy Policy must be part of the recruitment pack sent out.

All applications must be held securely under the terms of the GDPR policy.

All rejected applications must be disposed of securely 1 year after the closing date

All unsuccessful interviewee applications may be retained for a period of 1 year after the interview date in case of feedback requests, then must be disposed of securely

Successful interviewee applications should have 1 copy transferred to the personnel files, and all additional copies securely disposed of.

All application forms must state that the information provided will be handled in accordance with the GDPR

Unsolicited CV's should be deleted and the candidate should be informed

Personnel files

All documents pertaining to existing staff must be kept in a securely locked cabinet.

No data relating to staff will be shared with unauthorised personnel.

Times sheets, leave sheets, sickness records, medical reports and correspondence from the projects must be printed off, filed in cabinet and electronic versions deleted both in Core and at the team sites.

Records of previous staff must only be kept for a period of 6 years to facilitate reference requests, or redundancy or litigation queries.

Any record kept beyond 6 years for litigation purposes must be securely disposed of 6 months after the final verdict, unless on appeal

Records pertaining to staff being transferred out of the organisation under TUPE must be handed on to the new organisation.

All staff must be given a copy of the NBF Privacy policy

Relevant information pertaining to salaries, pension contributions and tax will be filed securely. Any information transmitted to a 3rd party should be in pdf format where possible or by secure data transfer

Funding Applications

All funding applications should be stored and transferred securely.

Funding applications must be disposed of securely 1 year after the deadline for applications has passed.

Basic information such as organisation name, funder and amount may be retained for monitoring purposes. Any information used for case studies must be anonymised unless you have the express permission of the individual involved.

Training/Events

Details of attendees at events and training courses must be disposed of securely after the event. Any information retained for monitoring purposes should be anonymised unless you have the express permission of the attendee to quote them (e.g. in case studies etc.).

Whilst you are encouraged to take photographs of events for marketing and publicity purposes, you must make sure that attendees are aware of the fact and have the opportunity to decline inclusion. At larger events it will be advisable to produce the Social media release (appendix c) and bring it to people's attention as they sign in

Volunteers

Any personal information held on volunteers must be held securely and not shared without the express permission of the volunteer.

Personal data must be disposed of securely 1 year after the volunteer has left service.

On recruitment, all volunteers must be given a copy of the NBF Privacy policy.

If any volunteer is to be given access to NBF files that may contain personal data they must be given a copy of the NBF GDPR Policy, the relevant Volunteer Privacy Notice and Information Governance policy (Healthwatch and Connect Well teams) to read, and must sign the statement (Appendix e) to say that they have read and understood them and agree to abide by them

e-mail

The general advice is to store essential e-mails for no more than 2 years, although business need may dictate that they are stored for a longer period, no more than 6 years.

However, common sense must apply – if you don't need the information contained in the e-mail delete it. If you do need the information contained but not the e-mail trail, then extract and store it securely elsewhere, inform the sender, and delete the e-mail.

If you receive an e-mail, active consent can be taken as read. However, it must be made clear, preferably in a Privacy notice on your website,(See Privacy Notice General Public in Sharepoint) that you will be retaining the email for no longer than necessary under Article 5 processing basis of *Legitimate Interests* and that the sender has the right to ask you to delete the e-mail.

If you are sending an e-mail, there must be sufficient information in your signature to inform the recipient of their rights and your intentions.

Telephone calls

If you write down personal details in the course of a telephone conversation with anyone from outside the organisation, you must inform the caller; if you intend to pass on those details, inform the caller.

Do not take more information than is necessary to you to perform your duty.

If the conversation involves a lot of information of a personal nature, you must inform the caller that you are recording it in accordance with Article 6 of GDPR, and preferably ask them to e-mail or write to you with the detail if at all possible

Social Media and Images

You must request a participant's consent before posting images on Social media or on the website (Appendix (c)

Subject Access

Subject Access Requests (SARs) must be directed in the first instance to the Data Privacy Officer. All SARs must be made in writing, they may be sent by electronic means such e-mail. The relevant team should then respond, under guidance, and take the following steps:

You must verify the identity of the person making the request, using ‘reasonable means’.

If the request is made electronically, you should provide the information in a commonly used electronic format.

You must provide a copy of the information free of charge. However, you can charge a ‘reasonable fee’ when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

Information must be provided without delay and at the latest within one month of receipt.

You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

The Data Privacy Officer must be kept informed of the actions you have taken to comply with the SAR

Appendix a

Data protection release

With your permission, the information you have provided will be stored and used for the following purposes:

1. For the distribution of newsletters, briefing papers, consultations, events, news and other information by North Bank Forum teams and partner/member organisations, to yourself.
2. For inclusion in [DESCRIPTION]
3. To support the work of [NAMES], allowing referrals to your organisation as appropriate
4. The contact and activity information provided will be made available to the public. This will include an entry on the North Bank Forum website and online maps [If relevant]. This will help to promote your organisation, its work and activities.

   Please note that

1. The data contained in these databases will not be passed on as a mailing list to other agencies.
2. The data contained in these databases will not be used for marketing or fundraising, beyond the activities outlined above
3. However, your contact details (organisation, address and phone number/e-mail) may be passed to individuals, partners and member organisations where relevant (e.g. when an individual or member organisation requires access to your services)
4. If you opt in below but wish to withhold particular information such as a personal address from the public domain, please contact [whoever maintains your lists] or indicate by putting WITHHOLD in the appropriate box.
5. By ticking the boxes below, you can opt in to each of the purposes outlined above. However, you can opt out at any time by e-mailing [whoever maintains your lists] or ringing [whoever maintains your lists]

Consent

I am happy to receive regular e-newsletters etc. from the [NAME]

yes		**no**	

I am happy for my information to be shared with [NAME – a separate box for EACH organisation you share the data with]

yes		**no**	

I am happy for the information to be publicly available on our website(s) and online maps

yes		**no**	

Data protection statement:

I understand that the information I have provided will be used only for the purposes specified on the form, and will be stored in accordance with the provisions of the Data Protection Act (1998) and the General Data Protection Regulations (2018)

Name Date:

Organisation:

Signature:

Please note, if returning this form electronically, the e-mail it is attached can be taken in place of the signature where appropriate and if so indicated

Please return this form to:

Appendix b

Sample Data Protection Release for volunteers

1. The personal data stored by [PROJECT NAME] is used to register you as a volunteer and administer the effective allocation of your skills and attributes within roles and opportunities available to you as part of [PROJECT NAME] delivery

2. The data we hold will not be passed on as a mailing list to other agencies.

3. The data stored by[PROJECT NAME] will not be used for marketing or fundraising,

4. However, your contact details may be passed to individuals, partners and member organisations with your permission to enable you to carry out your role as a volunteer

---

I understand that the information I have provided will be used only for the purposes specified, and will be stored in accordance with the provisions of the Data Protection Act (1998) and Article 6(a) of the General Data Protection Regulations (2018)

Name:

Date:

Signature:

Appendix c

Sample release social media

I am aware that NBF may be taking photographs of this event for marketing purposes and that images that include me may be uploaded to Social media, the website or in used in publications.

Yes I am happy for images that include me to be used this way

No, I do not wish to be included in any publicity materials

Name

Organisation

Date

Appendix d

Employee statement

Employee statement: Policies and Procedures

I have read and understood the Policies and Procedures of the North Bank Forum and agree to be bound by them.

Name:

Role:

Signature:

Date:

Employee Statement: Data Protection

I have read and understood the additional guidelines and policy covering Data Protection as it applies to NBF staff and volunteers, and agree to be bound by them.

Name:

Role:

Signature:

Date:

Information Governance Policy statement

I have read and understood the Information Governance Policy as it applies to NBF staff and volunteers, and agree to be bound by it

Name:

Role:

Signature

Date:

Appendix e

Volunteer Statement

Data Protection statement

I have read and understood the additional guidelines and policy covering Data Protection as it applies to NBF volunteers, and agree to be bound by them.

Name:

Signature:

Date:

Information Governance Policy statement

I have read and understood the Information Governance Policy as it applies to NBF volunteers, and agree to be bound by it.

Name:

Signature:

Date: