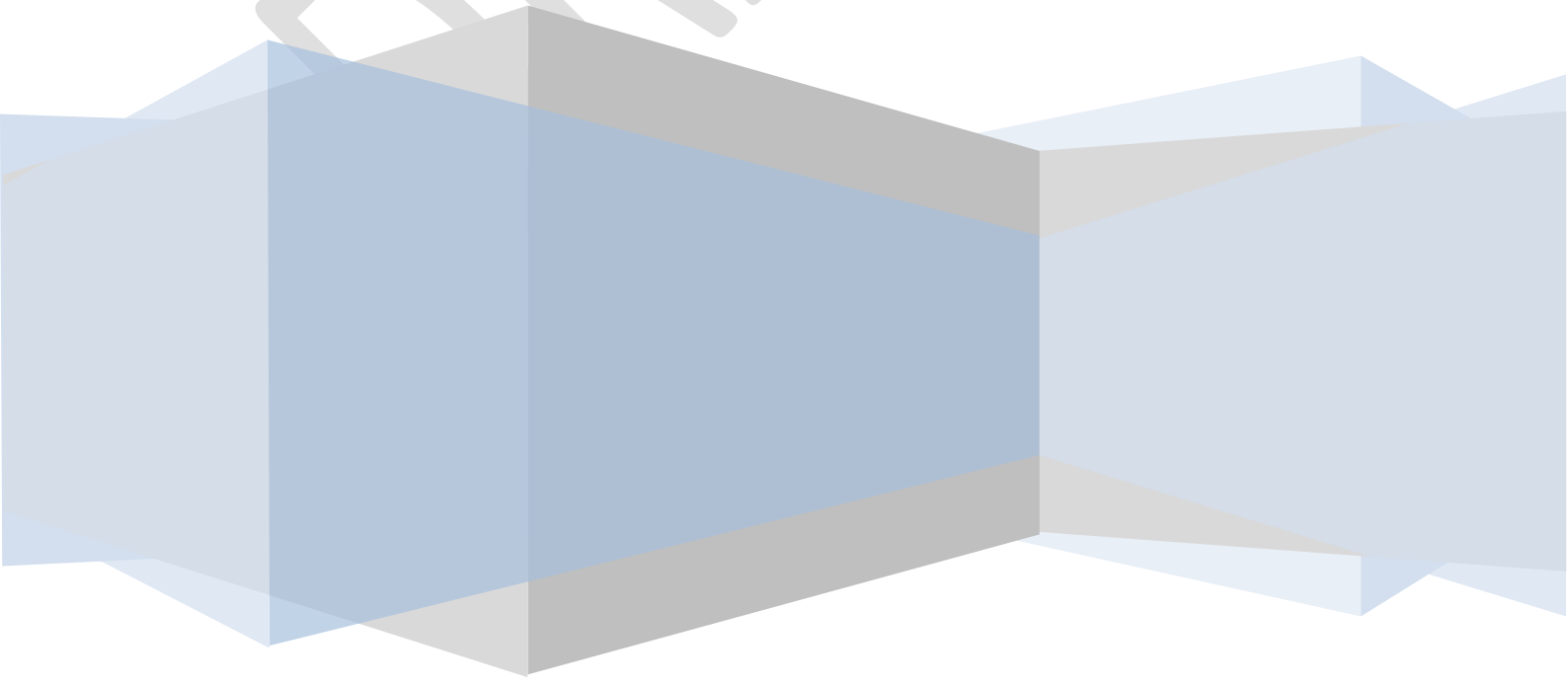
Northern Ireland Audit Office

NIAO DATA PROTECTION POLICY

Version 1.0

2018



Version	Date	Update Origin	Written by	Reviewed by
1.0		First Issue	N Connelly	J Campbell
2.0		Update		

TITLE	**NIAO Guide to Data Protection**
STATUS	**Final**
VERSION	**1.0**
AUTHOR	**N Connelly, Information Manager**
DATE OF ISSUE	
REVIEW DATE	
APPLIES TO	**All Staff**
DISTRIBUTION	**All Staff**
DOCUMENT LOCATION	**Circulars on huggett**

In brief

The General Data Protection Regulation (GDPR) replaces the Data Protection Act 1998 (DPA) and comes into force on 25 May 2018. It will become law in UK via the Data Protection Bill.

GDPR applies to "controllers" and "processors" of personal data[1]. A controller determines the purposes and means of processing the data; a processor is responsible for processing it on behalf of a controller – for example, an organisation (a data controller) may utilise the services of a marketing company or a payroll firm to perform work on the data controller's behalf.

Data Protection Principles – GDPR sets out six principles for processing personal data were established:

1. It will be processed in a fair and lawful manner;
2. It is collected for a specified purpose;
3. It is adequate and relevant
4. It is accurate and up-to-date;
5. It is kept no longer than is necessary
6. Data held has adequate security measures in place.

Lawful Basis – There are six lawful bases for processing data. No single basis is 'better' or more important than the others – which basis is most appropriate for an organisation to use will depend on the organisation's purpose and relationship with the individual.

For processing personal data for audit purposes NIAO will rely on the basis of our public task; for processing personal data for HR purposes, NIAO will rely on our legal obligation.

Individual Rights – GDPR has enhanced the entitlements of the individual – these are

- the right to be informed over how personal data is used;
- the right of access to their personal data;
- confirmation as to whether their personal data is being processed or not and how it is being processed;
- the right to rectification if data is inaccurate or incomplete;
- the right to erasure where there is no compelling reason for its continued processing;
- the right for an individual to restrict or "block" processing in certain circumstances;
- the right to data portability (across different services);
- the right to object to the processing of an individual's personal data; and

[1] 'Personal data", is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier

- rights in relation to automated decision making and profiling.

Accountability and Governance – NIAO is expected to have in place comprehensive but proportionate governance measures and implement good practice tools, such as privacy impact assessments and privacy by design. This is in order to protect all data subjects from privacy and data breaches.

Documentation – NIAO will ensure on an annual basis that our HR data is accurate and complete; all audit work has a personal data register in place; and all staff have provided notification of any personal data held on personal folders.

Data Protection by Design and Default - NIAO must show that we have considered and integrated data protection into our processing activities. We will therefore ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle (such as, building new IT systems for storing or accessing personal data, embarking on a data sharing initiative; or using data for new purposes). As part of this process, we are required to conduct Data Privacy Impact Assessments for all new projects to ensure privacy is an integral part of all our processes.

Data Protection Officer - As a public authority, we are required to appoint a data protection officer (DPO). The role of the DPO is to inform and advise the Office of its obligations to comply with GDPR and other data protection laws, to monitor compliance and be the first point of contact on all data protection issues.

Security of Personal Data - NIAO must guard against unauthorised or unlawful processing and against accidental loss, destruction or damage. This includes having appropriate encryption and passwords on laptops, secure retention of paper files and full compliance with the clear desk policy.

Data Breaches - We are also required to have a procedure in place for reporting personal data breaches. Included in these requirements is a need to identify what information has been breached, to notify ICO within 72 hours of becoming aware of the breach and inform those individuals without undue delay.

Non-compliance with any of these regulations can lead in fines of up to 20 million euro.

Introduction

The General Data Protection Regulation (GDPR) replaces all data protection legislation in all EU member states (including the Data Protection Act 1998 (DPA) and comes into force on 25 May 2018. GDPR will be incorporated into UK law via the Data Protection Bill.

While many of the themes, high level requirements and language of GDPR are not vastly different from the legislation it replaces, it does impose new obligations and stricter requirements on organisations covered by the Regulation.

Who does GDPR apply to?

GDPR applies to "controllers" and "processors". A controller determines the purposes and means of processing personal data; a processor is responsible for processing personal data on behalf of a controller – for example, an organisation (a data controller) may utilise the services of a marketing company or a payroll firm to perform work on the data controller's behalf.

GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods and services to individuals in the EU.

GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

What information does GDPR apply to?

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. The most obvious examples of this are name or an identification number. The GDPR also covers less obvious examples of personal data, such as an IP address, location data, mobile device identifier or factors specific to the physical, cultural or social identity of that person. These identifiers reflect changes in technology and the way organisations collect information about people.

GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

The Regulation also covers the circumstances under which the processing of "special categories of data" (also known as "sensitive personal data") may take place. The categories of data which are considered "sensitive" have been expanded from previous legislation – they now include genetic and biometric data as well as information about health, ethnic origin, sexual orientation, and political or religious beliefs.

Personal data relating to criminal convictions and offences are not included.

Data Protection Principles

Under GDPR, the data protection principles set out the main responsibilities for organisations. These principles, as set out in the DPA, remain but they have been condensed into six as opposed to eight principles within Article 5 of the GDPR. This states that personal data must be:

Principle 1: Processed fairly, lawfully and in a transparent manner in relation to individuals;

Principle 2: Collected for specified, explicit and legitimate purposes and not further processed for other purposes 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;

Principle 3: Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Principle 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;

Principle 5: Kept in a form that 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 GDPR in order to safeguard the rights and freedoms of individuals; and

Principle 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.

Article 5(2) of GDPR requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Lawful basis for processing

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate for an organisation to use will depend on the organisation's purpose and relationship with the individual.

These are broadly similar to the old conditions for processing, although there are some differences. The biggest change is for public authorities, who now need to consider the new 'public task' basis first for most of their processing, and have more limited scope to rely on consent or legitimate interests.

The GDPR also brings in new accountability and transparency requirements. Organisations need to make sure they clearly document their lawful basis so they can demonstrate compliance in line with Articles 5(2) and 24.

What are the lawful bases for processing?

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

(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.)

What is NIAO's lawful basis for processing?

NIAO's lawful basis for processing personal data for audit purposes is in our pursuit of our public task which has a clear basis in law. We are required to process personal data in order to comply with our legislative responsibilities as set out in The Audit (Northern Ireland) Order 1987; Government Resources and Accounts (Northern Ireland) Act 2001; the Audit and Accountability (Northern Ireland) Order 2003 and the Local Government (Northern Ireland) Order 2005. Effectively, our public task may be defined as a requirement to conduct our audits and economy, efficiency and effectiveness examinations as set out in our legislation.

Our processing of personal data is necessary for the performance of a task carried out in the public interest and in the exercise of the official authority vested in the C&AG, the Local Government Auditor and NIAO. 'Necessary' means that the processing must be a targeted and proportionate way of achieving our purpose. We do not need to have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.

It is important that we clearly identify the lawful basis of our processing as this has a direct impact on the rights that are available to individuals in respect of their personal data. Individuals' rights to erasure and data portability do not apply in circumstances where processing is carried out on the basis of public task; however, individuals do have a right to object.

NIAO processing of personal data is also necessary to comply with our **legal obligations.** Article 6(3) requires that the legal obligation must be laid down by UK or EU law. We do not need to have a legal obligation specifically requiring the processing activity – rather, our overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute. **This basis applies principally to our processing for HR and other personnel related matters**

Individual Rights

Under GDPR, the rights of individuals are provided for as follows:

Right to be informed- this encompasses the obligation to provide "fair processing information" as appropriate and emphasises the need for transparency over how personal data is used.

Right of access – individuals have the right to access their personal data. This right allows individuals to be aware of and verify the lawfulness of processing. Any individual, who makes a subject access request (SAR) in writing and on production of appropriate proof of identity, will be provided with a copy of any personal data held relating to them by NIAO.

Under GDPR, individuals have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information.

A copy of the information must be provided free of charge (there are some exceptions to this) and at the latest within one month of receiving the request.

A data subject is entitled to be provided with confirmation as to whether their personal data is being processed or not and if so:

- The purpose and legal basis for processing;
- The categories of personal data concerned;
- The recipients of the personal data;
- The period the data will be stored;
- The existence of any rights they have in respect of the data (for example rectification); and
- The existence of their right to complain to ICO.

A SAR can be refused if it is "manifestly unfounded" or excessive.

Right to rectification – GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete. The data must be rectified within one month of receiving the request.

Right to erasure - this is also known as the "right to be forgotten". The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances as set out below:

- 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; or
- The personal data is processed in relation to the offer of information society services to a child;

Under the GDPR, (and unlike DPA), this right is not limited to processing that causes unwarranted and substantial damage or distress.

Specific circumstances where the right to erasure does not apply, are as follows:

- 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;
- For archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- In the exercise or defence of legal claims.

The lawful basis of processing, therefore, can impact on which rights are available to individuals. In the case of NIAO, our lawful base for processing personal data for audit purposes is "Public Task": for that reason the right to erasure is not available to individuals for personal data used in performing our audit function. NIAO HR data is processed in accordance with a legal obligation and the right to erasure does not exist in that circumstance either.

Right to restrict processing – Individuals have the right to "block" or suppress processing of personal data. In those circumstances, as detailed below, a data controller can store the personal data, but not further process it:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data;
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you

are considering whether your organisation's legitimate grounds override those of the individual;
- When processing is unlawful and the individual opposes erasure and requests restriction instead; or
- If an organisation no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

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.

Some organisations in the UK already offer data portability through the midata[2] and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

This right to data portability 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.

The right to data portability does not apply to any personal data processed by NIAO.

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

Individuals must have an objection on "grounds relating to his or her particular situation."

Right 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

[2] midata is used to improve transparency across the banking industry by providing personal current account customers access to their transactional data for their account(s), which they can upload to a third party price comparison website to compare and identify best value. A price comparison website displays alternative current account providers based on their own calculations.

- Profiling (automated processing of personal data to evaluate certain things about an individual).

Accountability and Governance

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

Organisations are expected to put into place comprehensive but proportionate governance measures. Good practice tools such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

How do we demonstrate compliance with the accountability principle?

We will:

- Implement appropriate technical and organisational measures that ensure and demonstrate compliance. This includes internal data protection procedures such as staff training, internal audits of processing activities, and reviews of internal HR policies;
- Maintain relevant documentation on processing activities;
- Appoint a Data Protection Officer;
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - data minimisation;
    - pseudonymisation;
    - transparency;

- Allow individuals to monitor processing through their right to rectify their data; and
- Create and improve security features on an ongoing basis.

Documentation

The documentation of processing activities is a new requirement under GDPR. The GDPR contains explicit provisions about documenting processing activities. There are some similarities between documentation under GDPR and the information we provide to ICO as part of the registration process.

What NIAO needs to document ?

Under GDPR, the level of documentation required about an organisation is linked to its size. Organisations with 250 or more employees must document all processing activities. There is a limited exemption for organisations who fall below that threshold.

For NIAO, we only need to document processing activities that:

- Are not occasional; or
- Could result in a risk to the rights and freedom of individuals; or
- Involve the processing of special categories of data or criminal conviction and offence data.

To comply with this requirement we will document, in writing:

- Our processing of personal data for all HR purposes;
- Our processing of personal data for financial audit and public reporting purpose, using a personal data register for each audit;
- Communicate the purpose and results of our processing to audited bodies in the Letter of Understanding and RTTCWG respectively;
- Maintain records on data sharing and retention; and
- Make the records available to the ICO on request.

Annually we will ensure that

- HR data is accurate and complete;
- All audit work has a personal data register in place; and
- All staff have provided notification of any personal data held on personal folders.

The results of these annual compliance checks will be reported to SMT.

Data Protection by Design and Default

What is 'privacy by design'?

Under GDPR there is a general obligation to implement technical and organisational measures to show that, as an organisation, we have considered and integrated data protection into our processing activities. Privacy by design has always been an implicit requirement of data protection. It is an approach to projects that promotes privacy and data protection compliance from the start. The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:

- Building new IT systems for storing or accessing personal data;
- Developing legislation, policy or strategies that have privacy implications;
- Embarking on a data sharing initiative; or
- Using data for new purposes.

Benefits of taking a 'privacy by design' approach

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly;
- Increased awareness of privacy and data protection across an organisation;
- Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection legislation; and
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

How do we demonstrate that we comply with the 'privacy by design' principle?

- All our working practices should anticipate and prevent privacy invasive events before they happen. All staff must ensure any personal data is handled appropriately;
- Personal data should be automatically protected in any given IT system or business practice – password protection and anonymisation are essential considerations in this regard;

- There should be end-to-end security for personal data. Strong security measures are essential to privacy from start to finish. Data should be securely collected, retained and then securely destroyed at the end of the process in a timely fashion;
- Privacy by design should be embedded in all our business practices. Privacy should be an essential component of the process being delivered.
- We should provide assurances to all stakeholders that whatever the business practice or technology involved, it is operating according to the stated objectives.

Information technology allows us to protect privacy through methods such as removing personal identifiers from data, or by encrypting personal information in a manner so that it can only be viewed by those authorised to do so.

Privacy is good for any organisation – privacy should be treated as a business issue, not a compliance issue. In line with GDPR we must demonstrate accountability and transparency in or handling of personal data.

Security considerations are key in maintaining privacy of personal data. It is important that our physical and technological security measures are in place and implemented. We may put away records each evening but if they are placed in an unlocked cabinet, then the privacy of that information cannot be assured.

Data Protection Impact Assessments

Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. It's a documenting process which will allow any organisation to systematically describe and analyse its intended processing of personal data, helping to identify and minimise data protection issues at an early stage. An effective DPIA will allow organisations to reduce the associated costs and damage to reputation, which might otherwise occur - the use of DPIAs is an integral part of taking a privacy by design approach and will be applied in all future NIAO projects where personal data may be processed.

It is essential, then, that NIAO Data Protection Officer, is consulted at the planning stage for any new procedure or process to provide advice on the completion of a PIA.

Data Protection Officers

The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in some circumstances. The GDPR also contains provisions about the tasks a DPO should carry out and the duties of the employer in respect of the DPO.

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

Under the GDPR, you **must** appoint a DPO if you:

- Are a public authority; or
- 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.

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

- 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 supervisory authorities and for individuals whose data is processed (employees, customers etc).

What does the GDPR say about employer duties?

Employers must ensure that:

- **The DPO reports to the highest management level of the organisation** – NIAO DPO will report annually on compliance with data protection. DPO will also report any potential and actual personal data breach to SMT and NIAO ARAC as necessary.
- **The DPO operates independently and is not dismissed or penalised for performing their task.**

Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss,

destruction or damage. It requires that appropriate technical or organisational measures are used. Therefore, NIAO must ensure that it has:

- appropriate technical measures in place around encryption of laptops and password controls;
- Paper files stored and transmitted securely - all staff must also comply with the policy on Securing Hard Copy Information (MIC 05/15); and
- Full compliance with the clear desk policy. Compliance with this policy is tested with periodic security checks.

Personal Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Any organisation must:

- Identify what information has been breached, the numbers of records lost and the sensitivities of the breach;
- Notify the relevant supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of the breach;
- Inform those individuals without undue delay, if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms;
- Have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not there is a need to notify the relevant supervisory authority and the affected individuals; and
- Keep a record of any personal data breaches, regardless of whether they are required to notify.

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 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.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Examples

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.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, we should 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 you 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.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Example

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.

What information must a breach notification to the supervisory authority contain?

- a description of 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, including, where appropriate, the measures taken to mitigate any possible adverse effects.

When do individuals need to know about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned directly must be informed without undue delay. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

What does the GDPR require an organisation to do in response to a breach?

The requirement to notify the supervisory authority within 72 hours starts as soon as it is established that a breach has occurred. It is important that once any member of staff discovers they may have lost any personal data, they must contact the Office's emergency number as soon as possible, even if the potential breach is discovered outside working hours.

NIAO must record all breaches, regardless of whether or not they need to be reported to the ICO. The record should include the facts relating to the breach, its effects and the remedial action taken. This is part of our overall obligation to comply with the accountability principle, and allows ICO to verify our compliance with its notification duties under the GDPR.

As with any security incident, we will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

What will NIAO do in response to a potential personal data breach?

As soon as anyone becomes aware of a potential personal data breach, they must:

- Report the incident to their line manager and the DPO;
- DPO must be provided with all details of the case – how the breach has occurred, personal data affected and a list of individuals involved;
- DPO will prepare a report (with an initial assessment of the incident) for the Director of Corporate Services. In discussion with DPO, the Director of Corporate Services will make a decision on whether to notify ICO and if any individuals need to be notified
- All potential and actual personal data breaches will be reported to SMT
- Following each personal data incident, DPO will conduct a review of processes and report any lessons to be learned to SMT.