NALA
Data Breach Policy and Procedures

NALA
National Adult Literacy Agency
Áisíneacht Náisiúnta Litearthachta do Aosaigh

Policy area	GDPR
Document reference number	NALA/DBP02
Version	02
Document drafted by	NALA
Date Policy approved	29 April 2022
Policy to be reviewed	April 2025

Table of Contents

Introduction

National Adult Literacy Agency (NALA) is committed to its obligations under the General Data Protection Regulation (GDPR) to maintain a robust and structured program for compliance and monitoring. We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur, hence this policy states our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to the GDPR.

Aim of policy

The aim of this policy is to provide an overview of NALA's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees; ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

Who is covered by this policy?

This policy applies to all staff within NALA (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the agency in Ireland or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

Definitions

Term	Definition
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Personal Data	Any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special Category Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Data Subject	The individual to whom some personal data relates.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Officer	An appointed officer with responsibility for the Data Protection compliance of the organisation.
DPC	The Irish Data Protection Commission, (Statutory Authority)
GDPR	The General Data Protection Regulation (EU) 2016/679.
Third Party	A natural or legal person, public authority, agency or body other than the Data Subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Data Security & Breach Requirements

The definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Alongside our 'Privacy by Design' approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by NALA.

We carry out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments that assess the scope and impact of any potential data breach; both on the processing activity and the data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including but not limited to:

- Encryption of personal data
- Restricted access
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures to assess, review and evaluate the effectiveness of all measures in compliance with the data protection regulations
- Frequent and ongoing data protection training programs for all employees
- Staff assessments and regular knowledge testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information
- Reviewing internal processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal; it is rechecked and authorised by the Governance and Compliance Officer.

Data Management Objectives

- To adhere to the GDPR and Irish Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and to reduce the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in the GDPR
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect consumers, clients and employees; including their information and identity
- To ensure that where applicable, the Governance and Compliance Officer is involved in and notified about all data breaches and risk issues
- To ensure that the Data Protection Commission is notified of any data breach (where applicable) with immediate effect and at the latest, within 72 hours of the NALA having become aware of the breach

Breach Detection

Categories of Data Breaches

A ‘personal data breach’ is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Security breaches can be categorised according to the following three information security principles:

- **Confidentiality Breach**: where there is an unauthorised or accidental disclosure of, or access to, personal data.
- **Availability Breach**: where there is an unauthorised or accidental loss of access to, or destruction of, personal data.
- **Integrity Breach:** where there is an unauthorised or accidental alteration of personal data.

It should be noted that while these breaches may occur as separate incidents, depending on the circumstances, a breach may fall into more than one of the above categories.

Examples of Breaches

The following non-exhaustive list are examples of personal data breaches where a staff member is required to initiate the reporting process and begin documenting the breach:

- Loss or theft of personal data or equipment which stores personal data (e.g. personal information being misplaced or left in an uncontrolled environment).
- Equipment theft or failure.
- Unauthorised disclosure of personal data (e.g. correspondence sent to incorrect recipient(s); personal information not appropriately redacted before releasing documents in response to a Subject Access Request (SAR).
- Unauthorised use of, access to, or modification of personal data or information systems (e.g. users having inappropriate access rights to shared drive folders).
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s).
- Successful phishing attacks where information is obtained by deceiving the company who holds it.
- Temporary loss of availability due to events such as a fire or flood.

Data Processor Breaches

Where NALA has engaged a third-party service provider (processor), to perform processing on the company's behalf:

The processing activity carried out by the processor will be governed by a processing agreement in accordance with Article 28 (or Article 46 for international transfers) of the GDPR which includes a requirement for the processor to notify NALA of any breaches of data for which NALA is the data controller.

NALA will retain overall responsibility for the protection of personal data. However, the processor is required to assist NALA in ensuring compliance with its obligations including assisting NALA in securing breached data and notifying sub-processors engaged by the processor.

Processors engaged by NALA must commit to alerting NALA without undue delay, of all potential and confirmed breaches, which give rise to the risk of unauthorised disclosure, loss, destruction or alteration of personal data, where NALA is the controller of the compromised personal data.

Likewise, where NALA processes data on behalf of a controller, NALA must notify the controller without undue delay of all potential and confirmed breaches, which give rise to the risk of unauthorised disclosure, loss, destruction or alteration of personal data.

Data Breach Procedures & Guidelines

NALA has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

Breach Monitoring & Reporting

NALA has appointed the Governance and Compliance Officer as the person responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person and the relevant manager/CEO with immediate effect, whereby the procedures detailed in this policy are followed.

All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure

that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process must be recorded.

Breach Incident Procedures

Data Breach Identified

As soon as a data breach has been identified, it is reported to the direct line manager and the Governance and Compliance Officer immediately so that breach procedures can be initiated and followed without delay.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of the agency and is not about apportioning blame. These procedures are for the protection of NALA, its staff, learners, members, clients and third parties and are of the utmost importance for legal regulatory compliance.

The staff member and their line manager together will document (see Appendix 1) the incident with as much information as possible with the support of the Governance and Compliance Officer.

As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

Breach Investigation

The aim of the investigation is to determine the nature of the breach, contain the breach, the consequences for the data subject(s) involved, whether the requirement for notification the Data Protection Commission (DPC) or the data subject(s) has been triggered, and the mitigating or remedial actions to be taken.

Once a potential breach has been detected, the Governance and Compliance Officer will meet with the relevant personnel to discuss the required steps to secure the breach. NALA will prioritise securing the data that may have been breached. How this is achieved depends on the nature of the breach, for example:

Type of incident	Potential response
Email sent to wrong recipient(s) containing personal data	Ask recipient(s) to erase email from inbox and from their deleted items. Request confirmation from recipient
Loss/theft of IT equipment	Report theft to Gardaí, where relevant, and contact Office Manager to ensure equipment cannot be reconnected to network.
Accidental release of personal information in a response to an SAR	Ask recipient to return or confirm destruction of the record and replace the record with a copy where the personal information has been redacted.
Unauthorised access to data on internal systems	Contact the Office Manager or ERS (NALA's IT support) to request access denial

Speed is of the essence and contact should be made by the most appropriate method. Telephone is often the best way to communicate.

The Governance and Compliance Officer will consult with senior management to investigate and assess appropriate mitigating actions for the breach. Where required the NALA Board and/or external stakeholders may be consulted on a particular breach.

Risk Assessment

Once a potential breach has been detected and secured a risk assessment will be undertaken by NALA to determine the risk to the rights and freedoms of the affected data subject(s).

A 'high risk' occurs where the breach may lead to physical, material or non-material damage to the data subjects and may include instances of stress, discrimination, identity theft or fraud, financial loss or damage to reputation.

When assessing the severity of a breach, NALA will take guidance from a number of sources in order to determine the risk associated with the breach. NALA will refer to:

- The European Union Agency for Cybersecurity (ENISA) breach severity model. This document sets out a methodology for assessing the severity of a personal data breach
- The ENISA Breach Severity Tool spreadsheet (separate document on NALA SharePoint)
- European Data Protection Board (EDPB) breach notification document. This document provides practice-oriented, case-based guidance that utilises experiences gained by Statutory Authorities since the GDPR is applicable. Its aim is to help data controllers in deciding how to handle data breaches and what factors to consider during risk assessment.

NALA needs to consider the specific circumstances of the breach, including its severity and potential impact. The risk will also be evaluated on the basis of, at least, an objective assessment of the following criteria:

- The type of breach
- The nature, sensitivity and volume of personal data
- Ease of identification of data subjects
- Severity of consequences for data subjects
- Special characteristics of the data subject
- Number of affected data subjects
- Should authorities become involved

An assessment of such a breach may be aided by any previously conducted Data Protection Impact Assessments (DPIAs) of the processing activities affected by the breach.

Human Error

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee(s) held.

A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, but are not limited to:

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning (in-line with the Company's disciplinary procedures)

System Error

Where the data breach is the result of a system error/failure, ERS, NALA's 3rd Party IT providers, are to work in conjunction with the Office Manager and Governance and Compliance Officer to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form. (Appendix 1).

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident:

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from their tasks
- The use of back-ups to restore lost, damaged or stolen information
- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be changed immediately, and members of staff informed

Mitigate Risks

Once it has been established that a data breach has occurred, the Governance and Compliance Officer will take immediate and appropriate action to limit the breach. The steps taken will be dependent on the nature and cause of the breach e.g. human error, malware or phishing email. NALA will take guidance from the EDPB document on Data Breaches published in January 2021 to determine mitigation steps.

Breach Recording

NALA uses a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. To demonstrate compliance and accountability, NALA shall maintain a record of each personal data breach. Completed forms are logged in the Breach Incident Folder by the Governance and Compliance Officer on SharePoint and reviewed against existing records to ascertain patterns or reoccurrences.

In cases of data breaches, the Governance and Compliance Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

In documenting the breach, NALA will record at least the following details:

- Cause of the breach
- Description of the breach
- Effects and consequences
- Mitigating actions taken
- Reasons for not notifying a breach including reasons why the breach was not considered likely to result in a risk to the data subject(s)

NALA will retain proof of communications to the data subject regarding breaches to assist in demonstrating accountability and compliance. In circumstances where the Data Protection Commission is not notified, an explanation of the basis of not doing so must be retained.

A full investigation is conducted and recorded on the breach incident form, the outcome must be communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes. The Governance and Compliance Officer will keep an ongoing log detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk and investigation and recommendations for future work and/or actions.

Breach Notifications

If applicable, the Data Protection Commission (DPC) and the data subject(s) are notified in accordance with the GDPR requirements. The DPC protocols are to be followed and their online form available on the DPC website, should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

NALA recognises its obligation and duty to report data breaches in certain instances. All staff have been made aware of the agency's responsibilities and strict internal reporting lines have been developed to ensure that data breaches falling within the notification criteria are identified and reported without delay.

Notification to the Data Protection Commission

Under GDPR Article 33, NALA shall, where feasible, not later than 72 hours after having become aware of a personal data breach, notify the personal data breach to the Data Protection Commission (DPC), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The Working Party 29 states that as data controller, NALA, shall not be considered 'aware' of a breach until they have a reasonable degree of certainty that a security incident has occurred which has resulted in personal data being compromised. This allows NALA a short period of time to actively investigate potential breaches to assess if they are actual breaches.

The Data Protection Commission is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals.

Where applicable, the DPC is notified of the breach no later than 72 hours after NALA has become aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

Where a breach is assessed by the Governance and Compliance Officer and deemed to be **unlikely** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the DPC in accordance with Article 33 of the GDPR.

Notification Delay

Where the notification to the Data Protection Commission is not made within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay.

Information to be provided

Under Article 33(3) of the GDPR, the breach notification to be supplied to the Data Protection Commission shall include at least the following information:

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned
- The name and contact details of our Governance and Compliance Officer and/or any other relevant point of contact, for obtaining further information
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

When reporting a breach to the DPC we do so using the online form available on the DPC website. This form defines all of the information required.

Notification in Phases

Where further investigation by NALA is required, further information 'may be provided in phases without undue further delay and accompanied by reasons for the delay. As outlined under Articles 33 of the GDPR.

When NALA first notifies the Data Protection Commission, it will outline whether it intends to supply more information at a later stage. If it transpires during the investigation that the incident was contained and there was no breach, NALA will still notify the Data Protection Commission of this conclusion.

Delays could result in additional sanctions by the DPC and so should be avoided. Where a breach is confirmed but not all of the necessary reporting information is

available, NALA will submit the initial breach form within the 72 hours and indicate that an updated will be provided when additional information is known. Breach incident procedures are always followed, and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Data Protection Commission, if requested.

Notification to the Data Subject

Article 34 of the GDPR states that where a personal data breach is likely to result in a 'high risk' to the rights and freedoms of individuals, the controller shall communicate the personal data breach to the individuals 'without undue delay'. High risk can be assessed using the ENISA methodology and EDPB guidance referenced earlier in the document.

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

Contacting the Data Subject

NALA will aim to contact the data subject directly unless it would involve a 'disproportionate effort' in line with Article 34(3) of the GDPR. Where this is the case, a public communication or similar approach will be taken.

This communication will be a dedicated message and sent separately to other information such as newsletters or updates. NALA will choose a means of communication that maximises the chance of properly communicating information to individual data subjects.

Information to be provided

As outlined under Article 34 (2) of the GDPR, the breach notification to be supplied to the data subject by NALA shall:

- Be in clear and plain language; and
- Include at least the following information;
    - Description of the nature of the breach
    - The name and contact details of our Governance and Compliance Officer

and/or any other relevant point of contact where more information can be obtained

- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach, including measures to mitigate the breaches adverse effects

Conditions where Notification is not required

Under Article 34(3), the GDPR provides three conditions where a notification to an individual is not required in the event of a high-risk personal data breach.

1. **Technical and Organisational Measures**: NALA 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 (E.g. Encryption, data masking). However, even where data is encrypted, a loss of data may have negative consequences for data subjects where NALA retains no backups. In this regard, a notification to the data subject would be required as the breach affects NALA's ability to restore the availability and access to personal data.
2. **Subsequent Measures:** NALA has taken subsequent measures which ensure that the high risk to the rights of the data subject are no longer likely to materialise.
3. **Disproportionate Effort:** communication to the data subjects would involve disproportionate effort. In such an instance, as outlined above, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

These three conditions should be used with caution. Where they are relied on to restrict NALA's reporting obligations, the justification for making this decision should be documented and challenged by the Governance and Compliance Officer. If a previously perceived risk materialised despite meeting one of these conditions, the DPC would challenge NALA's justification for not notifying the affected data subject(s).

Breach Incident Review

Following containment of the initial breach, any outstanding mitigation actions will be completed. The Governance and Compliance Officer will conduct a full review of the cause of the breach and the subsequent actions taken. The review will ensure that the steps taken during the incident were appropriate and identify whether further actions are required to identify areas that may need to be improved to prevent the breach from occurring again. These actions may include reviewing systems or implementing policies and procedures.

Record Keeping

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Governance and Compliance Officer and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

Responsibilities

NALA will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

The Governance and Compliance Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups.

Related Documentation

Data Protection Policy
Subject Access Request Policy
Subject Rights Policy

Appendix 1 - Data Breach Incident Form

GOVERNANCE AND COMPLIANCE OFFICER /INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
TEL:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
BREACH NOTIFICATIONS:			
WAS THE SUPERVISORY AUTHORITY NOTIFIED?			**YES/NO**
IF YES, WAS THIS WITHIN 72 HOURS?			**YES/NO/NA**
If no to the above, provide reason(s) for delay			

WAS THE BELOW INFORMATION PROVIDED? *(if applicable)*	YES	NO
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Governance and Compliance Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
WAS NOTIFICATION PROVIDED TO DATA SUBJECT?	**YES/NO**	
INVESTIGATION INFORMATION & OUTCOME ACTIONS:		
DETAILS OF INCIDENT INVESTIGATION:		
PROCEDURE(S) REVISED DUE TO BREACH:		
STAFF TRAINING PROVIDED: (if applicable)		
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:		
HAVE THE MITIGATING ACTIONS PREVENTED THE BREACH FROM OCCURRING AGAIN? (Describe)		
WERE APPROPRIATE TECHNICAL MEASURES IN PLACE?	**YES/NO**	
If yes to the above, describe measures		
Investigator Signature: _____ Date: _____ Investigator Name: _____ Authorised by: _____		