NALA

Data Protection Policy

National Adult Literacy Agency

Áisíneacht Náisiúnta Litearthachta do Aosaigh

Policy area	GDPR
Document reference number	NALA/DP02
Version	02
Document drafted by	NALA
Date Policy approved	27 April 2022
Policy to be reviewed	April 2025

Contents

Introduction

The General Data Protection Regulation (GDPR) and the Irish Data Protection Legislation tells us and other organisations how we must handle data about people.

‘Data’ means any information about people we collect. ‘Data processing’ is a phrase used to describe all the different ways data is used and stored.

This Data Protection Policy tells you how NALA handles and protects any data we gather about you to make sure that we comply with these laws.

We gather data about:

- employees
- learners
- clients
- our members
- other individuals
- our suppliers.

This means that we control data and we are a ‘data controller’.

What data is covered by this policy?

Our policy covers all the data, including personal and sensitive details that we collect about people. It covers data held on paper and on computers.

We will treat all data with equal care.

Six ways NALA protects your data

There are six things we do to make sure we handle your data appropriately.

1. We are lawful, fair and clear

We will handle your data:

- in line with the law
- in a fair way
- in a clear way that everyone can understand.

Lawful

Generally, how we handle data is based on legislation under GDPR Articles 6.1 (a), (b), (c), and (f).

This means we will ask your permission to handle your data when necessary. You can withdraw your consent at any time.

However, to enter any contract with us, you must give us permission to handle your data. So, if you withdraw your consent to use any of your data, we must withdraw our services from you.

Fair

For data processing to be fair, we have to make certain data available to you.

We will only handle data in ways that people would reasonably expect us to do so, and we will not use your data in ways that might damage you unfairly.

We must do this if we got the data directly from you, or from other sources. You may have forgotten what information you gave us and wish to see what it was.

Clear

We will provide necessary data to you when you need it. When we provide data we make sure it is:

- detailed and specific
- clear and in plain language.

We make data available through our:

- websites
- forms
- publications.

2. We gather data only as needed to provide services

We design systems to collect data so we can gather and use it:

- only for the purpose for which we collect it
- so we can provide the service you have asked for.

This applies to:

- online forms
- hard copy documents
- other ways of collecting data.

Our employees must only accept a request for data from another organisation or person if it is directly related to the reason we collected the data in the first place. Even if the reason seems related, our staff must not reveal data unless it is why we originally collected your data.

If we need to give your data to another organisation or person we must first assess the impact this will have on you before sharing it and ensure the organisation also complies with GDPR.

This assessment is called a ‘Data Protection Impact Assessment’ (DPIA).

3. Accuracy

We will make sure any data we keep about you is accurate and up to date. We need to do this so we can provide our services.

You have the right to make sure the data we hold about you is accurate and complete.

We design the ways we collect data so that it is easy to update information when we get new data.

If we have provided data about you to third parties which is no longer accurate, we will give them the updated data.

However, we will not do this if it is impossible or requires significant time or effort to do so. For example, if you change your mobile number and we do not have any other contact data to reach you.

4. We will keep your data only for as long as needed

The legislation says we should keep any data that identifies you only for as long as we need it to provide our service to you.

We put in place policies and procedures to make sure that we keep any data that identifies you for the least amount of time needed so we can operate effectively.

We have systems in place to destroy or remove data that identifies you after we no longer need it.

5. Security

The law requires us to use technical and organisational security measures when handling data to protect against:

- unauthorised or unlawful access
- accidental loss, destruction or damage.

We have put in place the necessary measures to do this.

6. Accountability

We are accountable for, and able to show how we comply with the data protection legislation. We do this by using appropriate records and systems for handling your data.

Your data and your rights

We design and maintain appropriate policies, procedures and staff training to make sure we fulfil the legal rights related to your data.

‘Access’ your data

(Right of access by the data subject, GDPR, Article 15)

You have the right to access any of your data which is being processed by us.

We put in place ways of working that make sure when you ask for details of data we hold about you, we can find and provide the data. We do this within the time allowed in the legislation.

‘Rectification’ – correct your data

(Right to rectification, GDPR, Article 16)

If you think we hold inaccurate or incomplete data about you, you have the right to ask us to correct it.

We have systems in place to make sure that we can correct data about you that is inaccurate.

‘Erasure’ – have your data wiped from our records

(Right to erasure [‘right to be forgotten’], GDPR, Article 17)

You have the right to ask us to delete or remove your data where there is no reason for us to keep it. If this is possible we will do so.

In some cases, there may be some legal reason why we cannot remove your data. For example, where we must:

- perform a task in the public interest
- keep your data because it is related to a legal claim
- keep your data for our archive.

‘Restriction’ – challenge how we use your data

(Right to restriction of processing, GDPR, Article 18)

If you ask us to limit how we use your data, we will do so if the following circumstances apply. You argue that:

- the data we hold about you is inaccurate
- NALA no longer needs the data, but you do
- you have already lodged an objection to NALA about using your data.

You may also argue that processing your data is unlawful. You may be against us wiping out your data, but ask us to restrict its use instead.

How we go about this

We put in place and maintain appropriate procedures. They enable us to assess if your request to restrict the processing of your data can be put in place. We will write to you:

- confirming we received your request
- if we can carry out your request
- when we have carried out your request.

If we later decide to use your data again, we will first write to you to let you know.

‘Portability’ – you can reuse data in more than one organisation

(Right to data portability, GDPR, Article 20)

You have the right to get and reuse your data across different organisations.

Where we collect your data with your consent or through a contract, you have a right to receive this data from us in electronic format. This allows you to move, copy or transfer data easily from one IT environment to another. It makes this safe and secure and your data easier to use. You can then give this data to a data controller in another organisation.

We will put in place appropriate procedures so that we transfer only the relevant data.

‘Object’ – you can object to us using your data

(Right to object, GDPR, Article 21)

You can object to us using your data. But we may still use it if we:

- can show compelling reasons why we need to do so
- can show we need to use your data in the public interest
- need your data to defend legal claims.

However, we will stop using your data if you tell us you object to us doing so for:

- direct marketing
- scientific research
- historical research
- statistical analysis.

If we need to use your data in the public interest for scientific or historical research or statistical analysis we will make sure that you cannot be identified. This is known as anonymisation.

‘Opt out’ – we don’t use ‘automated decision making’ but if we ever do, we will ask you first

(Right to opt out of automated individual decision-making, GDPR, Article 22)

Sometimes when organisations hold data about you, they use an automated decision system to decide things about you. However, if this type of decision would have a legal or significant effect on you, you can tell the organisation not to do so.

Currently we do not use automated decision making. If we ever decide to use your data in this type of system in the future, we will tell you in advance and give you the right to object.

Right to complain

If you wish to complain about how we use your data, you can contact our Governance and Compliance Officer.

The Governance and Compliance Officer will work with you to resolve your complaint. If you are not satisfied with how we resolved your complaint, the Officer will tell you about your right to bring your complaint to the Data Protection Commission. They will also give you the appropriate contact details.

Our responsibilities

‘Data controller’

NALA is considered a ‘data controller’.

A data controller is responsible for deciding how to use the data of its:

- clients
- staff
- stakeholders.

Stakeholders are people with an interest in an organisation and or its work.

We are committed to complying with the data protection legislation.

Technical and organisational systems

We have technical and organisational systems to manage your data. We have designed these to make sure we can protect your data. We update these systems as needed.

These systems also mean that we can clearly show how we use your data appropriately.

How the systems work

Security

We have put in place high security standards to protect your data.

Access

Only those who have the appropriate authorisation may access your data.

Backup

If there is ever an incident affecting our systems, we can restore the availability and access to data in a timely manner.

Constant vigilance

We regularly test, assess and evaluate how effective our organisational and technical measures are.

‘Records’ – keeping details of how we use data

(Records of processing activities, GDPR Article 30)

We will keep a record of how we use data as required by the legislation. We will review this at least once a year and make it available to the Data Protection Commission on request.

If there are any significant changes to an existing process or if we put in place a new process, we will let the relevant manager know so they can update the records.

Type of data we have on record

Name and contact details of:

- the data controller or joint controller
- controller’s representative
- relevant contact person.

We also keep a record of:

- the types of business systems we use
- categories of data we hold
- why it is legal for us to use data in the way that we do
- how long we can keep each type of data for
- when and why we share data with another organisation

- when we have transferred data to a third country, and what country that is
- the type of technical and organisational security measures we have put in place.

Our systems are designed to protect your data

(Data protection by design and default, GDPR Article 25)

When we are planning to introduce new systems or technologies, one of the first things we do is decide how to make sure we can continue to protect data.

The European Data Protection Board (EDPB) encourages data controllers like NALA to plan their systems in this way.

For example, all our new network folders are accessible only to those who need access to carry out their role in the organisation.

In this way, our technical and organisational systems protect the rights and freedoms of people whose data we have.

How we share data with other organisations

('Processor' and 'Transfers subject to appropriate safeguards', GDPR, Articles 28 and 46)

We will not share your data with any other organisation unless there is lawful reason for us to do so or to provide you with the service you have requested. We will seek your consent to share your information with another organisation.

Before we share any data with any other organisation, we put a written agreement in place. It includes how this data will be handled. By 'third party' we mean anyone or organisation, whether a part of NALA or outside NALA, who manages data on our behalf.

The agreement states:

- why data needs to be shared between us and a third party
- the right to terminate processing that we or the third party can take

- the third party may not transfer data to any other person or organisation
- if the third party is asked for data, they will provide it to us
- the right for us to audit the data that the third party holds.

Transfer of data outside of the European Economic Area

We will only transfer your data outside of the European Economic Area (EEA) if we can make sure it will be protected appropriately.

In June 2021, the European Commission adopted new Standard Contractual Clauses (SCCs) to do with appropriate safety for transferring data outside the EEA.

Before we undertake to transfer any data or to put new SCCs in place, we will conduct a 'Transfer impact assessment'. This will make sure that the SCCs are effective. If we find they are not effective, we will make sure that they are changed to reach the required standard.

If our security fails and there is a 'data breach'

A 'data breach' is a gap in security that leads to the accidental or illegal destruction, loss, alteration, unauthorised disclosure of, or access to data. An example of a breach is when correspondence is sent to an unauthorised third party.

We regard any loss of data in paper or digital form to be a data breach.

If there is a suspected data breach, our employees must notify the Governance and Compliance Officer. The senior management team along with the Governance and Compliance Officer will assess the severity of the breach. Where appropriate they will notify the Data Protection Commission within 72 hours.

Where a breach is likely to result in a high risk to the rights and freedoms of the people whose data has been compromised, we will notify them about the breach.

We assess new data gathering systems

We have a system for assessing the impact of all new types of data processing. This is called a ‘Data protection impact assessment’ (DPIA). We will share a copy of the assessment with our Governance and Compliance Officer. They will review the DPIA and provide advice where required.

If we cannot find ways to reduce any high risks identified in a DPIA, we will consult the Data Protection Commissioner before we begin using the new system.

Record keeping

We keep logs of relevant data protection related events, for example:

- if you ask us for any of your legal rights discussed in section ‘Your data and your rights’ to be respected (this is called ‘invocation of subject rights’)
- when data is used inappropriately
- when we carry out an assessment to see if we need to do a Data Protection Impact Assessment (DPIA).

Responsibilities of staff and others

Anyone who processes data on our behalf must comply with this data protection policy. All records created on our behalf belong to us.

Anyone who handles data we hold must read, understand and accept all our:

- data protection policies
- procedures
- guidelines.

They must also make sure that when they access, manage and control data as part of their daily duties, they do so in line with data protection requirements.

Everyone who handles data on our behalf must also make sure their department complies with our data protection rules.

Consequences of failing to comply

We take compliance with this policy very seriously. If we fail to comply, it puts individuals and the organisation at risk. Individuals who fail to follow our data protection policies may be subject to disciplinary procedures.

If staff consider that this policy has not been followed, they should raise the matter through their manager.

Related documents

- NALA Subject Access Request Policy
- NALA Data Subject Rights Policy
- NALA Data Breach Policy