Polasaithe
Naíonra Céimeanna Beaga

Polasaí 49: EMPLOYEE PERSONAL DATA PROTECTION POLICY

Gleann Aibhne,

Br. An Ghoirt,

Inis,

Co. an Chláir.

Stiúrthóir: Katie Uí Chaoimh, Fón: (086) 2114881

r-phost: naionragmc@gmail.com

Suíomh gréasáin: www.gmci.ie/naionra

Version	1.0
Date	Nov 2018
Policy Number	Policy Number 49
Owner	Naíonra Céimeanna Beaga
Validity and document management	This document is valid from Nov 1 2018. The owner of this document is the Owner / Manager, who must check and, if necessary, update the document at least once a year. This policy was adopted by Naíonra Céimeanna Beaga on 1 Nov 2018. Signed by: **Katie Uí Chaoimh;** Príomh Stiúthóir on behalf of Naíonra Céimeanna Beaga

Table of contents

1. Introduction

Naíonra Céimeanna Beaga strives to comply with applicable laws and regulations related to Personal Data protection in Ireland. This policy document regulates the management of employees Personal

Data that Naíonra Céimeanna Beaga processes. This policy provides rules and procedures which apply to all individuals within Naíonra Céimeanna Beaga, aimed at ensuring that employee Personal Data is processed and protected properly at all time

2. Who is this policy for?

This Policy applies to the processing of employee's personal data by any individual within or associated with Naíonra Céimeanna Beaga.

All employees either permanent or temporary, all contractors, all volunteers and students must read and understand this document, so they are fully aligned with the policy of Naíonra Céimeanna Beaga.

3. Reference documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Irish Data Protection Act, 1988 and Amended Act 2003

4. Definitions

There are certain legal documents that are relevant to this policy and we refer to these documents throughout. For your information these documents are listed below:

Personal Data

Any information relating to an identified or identifiable natural person 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, mental, economic, cultural, or social identity of that natural person. Personal Data includes a natural person's email address, telephone number, biometric information (such as fingerprint), location data, IP address, health care information, religious beliefs, Social Security number, marital status etc.

Sensitive Personal Data

Particularly sensitive in relation to fundamental rights and freedoms, where disclosure of such data could lead to physical damage, financial loss, damage to the reputation, identity theft or fraud or discrimination etc. Sensitive personal data usually includes but not limited to personal data revealing racial or ethnic origin, political opinion, religious or philosophical belief, or trade union membership, as well as genetic data, biometric data (fingerprint) for the purpose of uniquely identifying a natural person, and data concerning a natural person's health or sexual orientation.

Processing

An operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure, transmission, dissemination, restriction, erasure, or destruction of the data.

Data Controller

The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purpose and means of the Processing of Personal data.

Data Processor

A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

5. General Principles for Processing Employee Personal Data

Lawfulness, fairness, and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

There are three components to this principle; Lawfulness, Fairness and Transparency and they are all linked. The person must be told what processing will occur (Transparent), the actual processing must match this description (Fair), and finally the processing must match one of the six purposes specified in the GDPR (Lawful). When it comes to (Lawful) Naíonra Céimeanna Beaga relies on a GDPR fundamentals which are contractual and consent for processing employee's data.

Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

We must define up front what personal information we collect, how it is going to be used, for what purpose and we must limit using that information for that purpose(s) only.

We do that through our privacy notice, our terms and conditions and our consent forms.

For example, if we collect personal information from an employee and they have consented to that information being used as part of their employment I cannot use that information for any other purpose.

Data minimisation

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Only collect/hold enough data to carry out the process, don't collect/hold what you don't need. Keep it minimal.

Accuracy

Personal data must be accurate and, where necessary, kept up to date.

Any data that is being held needs to be accurate. Naíonra Céimeanna Beaga strives to keep the personal information they hold up to date and accurate. Data Subjects, can request any information held on them by Naíonra Céimeanna Beaga as this is their right, they can also request correction or completion of information relating them (See Data Subject Access Request Procedure).

Storage period limitation

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.

If the information is no longer required it should be securely disposed of. You should refer to the "Data Retention Policy' and the "Appendix – Data Retention Schedule" for information on why we keep data and for how long. They take into account the legal and contractual requirements and retention periods for information.

Integrity and confidentiality

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

In summary, every employee does not need access to the personal information that Naíonra Céimeanna Beaga collects. Only those that require access should have it. The physical security of the filing cabinets and rooms are to be considered and access to any electronic devises that hold personal data should be restricted accordingly.

Accountability

Naíonra Céimeanna Beaga is responsible for and must be able to demonstrate compliance with the principles outlined above.

If a third-party contractor, for example, a dance teacher, provides Naíonra Céimeanna Beaga with services, Naíonra Céimeanna Beaga have a contract of services with that third-party provider, that contract must include processes that outline that any personal information processed by the third party is being done so in compliance with the six principals outlined above. This is very important as Naíonra Céimeanna Beaga remain responsible for the personal data even if the third party are responsible for a data breach.

6. Legitimate Purposes for Processing Employee Personal Data

Naíonra Céimeanna Beaga may process employee Personal Data for legitimate purposes which include but not limited to:

Management. This purpose includes human resource management activities carried out during recruitment or the performance of an employment contract, such as interviews, termination of employment, attendance, performance management, compensation and benefits, training, employee services, health and occupational safety, and other activities for the purpose of human resource management or protecting the vital interests of employee.

Operations. This purpose includes business activities such as managing travel and expenses, managing company assets, providing IT services, information security, conducting internal audits and investigations, fulfilling the obligations of business contracts, and preparing for legal litigation, etc.

Compliance with the law. The Processing of employee Personal Data in order to comply with a legal obligation, for example: Garda vetting, police vetting, confirmation of qualifications etc.

7. Requirements for the Processing of Employee Personal Data

Any processing of Naíonra Céimeanna Beaga employee Personal Data by individuals must be for a legitimate purpose, and must comply with the following requirements:

Notification to Employees

For the purpose of transparency of employee Personal Data Processing, when Naíonra Céimeanna Beaga collects the Personal Data of an employee, the employee should be notified of the types of data being collected, the purpose and types of Processing, the employee's rights, and the security measures taken to protect the Personal Data. Notification may take the form of the publication or updating of statements on the protection of employee Personal Data, for example: the insertion of a privacy notice in employment contracts by the Employer.

Employee Choice and Consent

In principle, Naíonra Céimeanna Beaga may Process employee Personal Data for a legitimate purpose as an employer and generally it may do so without obtaining the consent of the employee, to improve the efficiency of internal operation.

Human resource management activities such as interviews, on boarding, termination of employment, attendance, compensation and benefits, employee services, health and occupational safety may involve the Processing of Sensitive Personal Data. The employer shall seek consent where applicable.

Naíonra Céimeanna Beaga must collect employee Personal Data for legitimate purposes and must comply with the principle of Data Minimisation. If the Personal Data of a job candidate or employee is collected from a third party (e.g. recruitment or background check agencies), Naíonra Céimeanna Beaga must make best efforts to ensure that the third party obtained the Personal Data by legitimate means.

No individual may collect Personal Data of job candidates or employee in a way which is inconsistent with the law or business ethics.

Use, Retention, and Disposal

Naíonra Céimeanna Beaga must use, retain, and dispose of employee Personal Data in a manner which is consistent with the notification to the employee. It must also ensure its accuracy, integrity, and relevance. They must take appropriate security measures to protect the employee Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized access, or disclosure according to Information security policy and other documents that describe data security.

Company individuals must not unlawfully destroy or alter employee Personal Data. They must not access, sell, or provide employee Personal Data to any third party unlawfully or without authorization.

Disclosure to a Third Party

When Naíonra Céimeanna Beaga needs to disclose employee Personal Data to a supplier or other third party (accountant for example) they should seek to ensure that the supplier or other third party will provide security measures to safeguard employee Personal Data that are appropriate. They should also require the third party to provide the same level of data protection as Naíonra Céimeanna Beaga by contract or agreement.

Employee Access

Naíonra Céimeanna Beaga must provide reasonable means for employees to access Personal Data held about them and allow employees to update, correct, erase, or transmit their Personal Data if appropriate or required by law. When responding to an employee request for access, Company individuals may not provide any Personal Data until they have verified identity of the employee. The Company needs to make sure that they know the identity of the person making the request before they can send the personal data to the individual.

Cross-border transfer of Employee Personal Data

Before transferring Personal Data out of a country, HR departments and individuals must consider whether the cross-border transfer is necessary or legal.

When transferring employee personal Data out of the European Economic Area, the transferred and the transferee must have signed a data transfer agreement in compliance with EU regulations and Cross Border Data Transfer Policy. The transfer must provide adequate protection for the data transferred in accordance with the data transfer agreement.

8. Responsibilities

The Owner/Manager is responsible for the management of employee Personal Data protection.

9. Response in the Event of Non-compliance

Any person who has knowledge of a data breach involving employee Personal Data should report it to the relevant persons within Naíonra Céimeanna Beaga . When is necessary to report the data

breach outside the Company, the Personal Data Breach Policy will be followed.

10. Accountability

Any individual who breaches this Policy may be subject to internal disciplinary action (up to and including termination of their employment); and may also face civil or criminal liability if their action violates the law.

11. Exceptions and Variations

Company individuals should also refer to this Policy when Processing the Personal Data of other personnel. "Other personnel" includes: (1) individuals seeking employment at Company; (2) individuals who have previously been employed by Company.

12. Owner and Contacts

The Owner/Manager is the owner of this Policy and must interpret and manage it.