Document Control

Document Number

LGTPOL002/2024

Author

Position	Name
Information & Reporting Officer	Jessie Shea

Stakeholders and Other Contributors

Position	Name
External Consultant	PrivacyEngine

Policy Origins

New	Legacy
x	

Revision History

Version	Issue Date	Author/Editor	Description/Summary of Changes
1.0	11 Sept 2024	Information & Reporting Officer	New

Reviewed By

Version	Name	Position	Review Date
1.0	Katherine Harford	Executive Director	11 September 2024
1.0	Trish Hurley	Infant Mental Health and Wellbeing Coordinator	11 September 2024
1.0	Grace Walsh	Speech, Language and Early Years Coordinator	11 September 2024

Approvals

Version	Issue Date	Approval Body	Approval Date	Effective Date
1.0	12 September 2024	Board of Directors	19 September 2024	19 September 2024

Data Protection Policy & Procedures

Contents

1. Policy Statement

Let's Grow Together! Infant & Childhood Partnerships CLG (Let's Grow Together, "The Company", "we", "our" or "us") needs to collect personal information (or data) to effectively carry out our everyday business functions and activities and to provide our programmes and services. Data is collected from: families (including children); service providers who join our programmes and services; and employees, including students, volunteers, and prospective employees. Information collected from families and service providers accessing our programmes and services includes (but is not limited to): name; address and contact details; date of birth; demographic information; medical, health, and/or behavioural information about children; and records from programme attendance. Information collected from employees includes (but is not limited to): employment information; bank and financial details; and education.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), Irish data protection laws and any other relevant the data protection laws and codes of conduct (herein collectively referred to as "the data protection laws").

The Company has developed policies, procedures, controls, and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures, and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a 'Privacy by Design' approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2. Purpose

The purpose of this policy is to ensure that the Company meets its legal, statutory, and regulatory requirements under the data protection laws, and to ensure that all personal and special category information is processed compliantly and, in the individuals' best interest.

The data protection laws include provisions that promote accountability and governance and as such the Company has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third parties on the responsibilities of handling and accessing personal data and data subject requests.

3. Scope

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

3.1 Definitions

- ***"Consent"*** of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them and/or the children they are a legal guardian of
- ***"Data controller"*** means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law
- ***"Data processor"*** means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller
- ***"Data protection laws"*** means, for the purposes of this document, the collective description of the GDPR and any other relevant data protection laws that the Company complies with
- ***"Data subject"*** means an individual who is the subject of personal data
- ***"GDPR"*** means the General Data Protection Regulation (EU) (2016/679)
- ***"Personal data"*** means 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
- ***"Processing"*** means 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
- ***"Recipient"*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing
- ***"Supervisory Authority"*** means an independent public authority which is established by a Member State
- ***"Third Party"*** means a natural or legal person, public authority, agency, or body other than the data subject, under our direct authority

3.2 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (EU) (2016/679) came into force for all EU Member States on 25th May 2018. The GDPR applies directly to Member States. As the Company processes personal information regarding individuals (data subjects), we are obligated under the GDPR to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

3.2.1 Personal Data

Information protected under the GDPR is known as "personal data" and is defined as:

"Any information relating to an identified or identifiable natural person; 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."

The Company ensures that a high level of care is afforded to personal data falling within the GDPR's 'special categories', due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that:

"Processing of 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 shall be prohibited – unless one of the Article 9 clauses applies."

3.2.2 The GDPR Principles

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')
c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
d) 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 ('accuracy')
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of

the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

f) 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 ('integrity and confidentiality').

Article 5(2) requires that '*the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles*' ('accountability') and requires that firms show how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

3.3 The Office of the Data Protection Commissioner (DPC)

The DPC is an independent regulatory office whose role is to uphold information rights in the public interest. The legislation they have oversight for includes:

- The Data Protection Act 2018
- The General Data Protection Regulation 2018
- The e-Privacy Regulation 2021

The DPC's mission statement is "*to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals*" and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws, the DPC, as Ireland's data protection supervisory authority, must oversee, enforce, and respond to complaints with regard to the data protection laws for data subjects and organisations within Ireland.

The Company has a Data Protection Officer, who is registered with the DPC.

3.4 Data Protection Officer (DPO)

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements, and responsibilities on firms to appoint a DPO and specifies the duties that the Officer themselves must perform.

A DPO must be appointed by a firm where:

- The processing is carried out by a public authority or body (except for courts acting in their judicial capacity)
- The core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- The core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

The Company has appointed a designated DPO, and we have done so in accordance with the GDPR requirements and have ensured that the assigned person has an adequate and expert knowledge of data protection law. They have been assessed as being fully capable of assisting the Company in monitoring our internal compliance with the Regulation and

supporting and advising employees and associated third parties with regard to the data protection laws and requirements.

4. Objectives

We are committed to ensuring that all personal data processed by the Company is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical, and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The Company has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

The Company ensures that:

- We protect the rights of individuals with regard to the processing of personal information
- We develop, implement, and maintain a data protection policy and procedure and training program for compliance with the data protection laws
- Personal data is only processed where we have verified and met the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations, and how they apply to their specific role and the Company
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing, and reporting any breaches or complaints with regard to data protection
- We have appointed a DPO who takes responsibility for the overall supervision, implementation, and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- We store and destroy all personal information in accordance with our Data Retention and Erasure Policy and Retention Register – Data Retention Schedule which has been developed from the legal, regulatory, and statutory requirements and suggested timeframes
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws and are provided with the Article 13/14 information disclosures in the form of a Privacy Notice

5. Governance Procedures

5.1 Accountability and Compliance

Our main governance objectives are to:

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all employees
- Identify key stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support, and budget to perform the role

The technical and organisational measures that the Company has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

5.2 Privacy by Design

We operate a 'Privacy by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems, and activities. We have developed controls and measures, that help us enforce this ethos.

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be '*limited to what is necessary*', which forms the basis of our minimalist approach.

Our systems, employees, processes, and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose, and only retain data for as long as is necessary. For example, data collection forms only have the fields that are relevant to the purpose of collection and subsequent processing. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Anonymisation

We utilise anonymisation on family records to store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (personal identifiers).

5.3 Legal Basis for Processing (Lawfulness)

At the core of all personal information processing activities undertaken by the Company, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

Data is only obtained, processed, or stored when we have met the lawfulness of processing requirements, where:

- The data subject or legal guardian has given consent to the processing of their personal data for one or more specific purposes

- Processing is necessary for compliance with a legal or contractual obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child)

5.3.1 Processing Special Category Data

Special categories of Personal Data are defined in the data protection laws as:

'Processing of 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 shall be prohibited – unless one of the Article 9 clauses applies.'

Where the Company processes any personal information classed as special category, we do so in accordance with Article 9 of the GDPR.

We will only ever process special category data where:

- The data subject or legal guardian has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for compliance with a legal or contractual obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child)

Where the Company processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing. Measures include:

- Verifying our reliance on Article 9(1) GDPR prior to processing
- Having an appropriate policy document in place when the processing is carried out, specifying our:
    - procedures for securing compliance with the data protection laws principles
    - policies as regard the retention and erasure of personal data processed in reliance on the condition
    - retention periods and reason (i.e. legal, statutory etc)
    - procedures for reviewing and updating our policies in this area

5.3.2 Records of Processing Activities

As an organisation with less than 250 employees, the Company does not maintain records of our processing activities, per GDPR Article 30.

5.4 Third-Party Processors

GDPR Article 4(10) defines a third party as '*any 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.*'

We do not use third-party processors.

5.5 Data Retention and Disposal

The Company have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts, and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data in all instances.

Please refer to our Data Retention & Erasure Policy for full details on our retention, storage, and destruction processes.

6. Data Protection Impact Assessments (DPIA)

The Company does not currently carry out any processing activities that are defined as requiring a DPIA. We monitor all activities against the GDPR Article 35 requirements, and will develop DPIA procedures should they become necessary.

7. Data Subject Rights Procedures

7.1 Consent and the Right to be Informed

The collection of personal and special category data is a fundamental part of the programmes and services offered by the Company and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws. The Company maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data.

The data protection law defines consent as; '*Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*'.

Where processing is based on consent, the Company have reviewed and revised all consent mechanisms to ensure that:

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (in fine detail), and easy to use and understand
- Pre-ticked, opt-in boxes are never used

- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We have ensured that withdrawing consent is as easy, clear, and straightforward as giving it
- Consent withdrawal requests are processed immediately and without detriment
- For special category data, the consent obtained is explicit (stated clearly and in detail, leaving no room for confusion or doubt) with the processing purpose(s) always being specified

Informed consent to be contacted is obtained from families via signing our paper registration form or checking the box and writing their name on our online registration form. Informed consent for all other activities is obtained from families via signing our paper consent form or checking the box and writing their name on our online consent form.

7.1.1 Information Provisions

Where personal data is obtained directly from the individual (i.e. through consent, by employees, written materials and/or electronic formats), we provide the below information in all instances, in the form of a Privacy Notice:

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our DPO
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1) "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party", details of the legitimate interests
- The period for which the personal data will be stored
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority

7.2 Privacy Notice

Our Privacy Notice provides individuals with all the necessary and legal information about how, why, and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The Notice is the client facing policy that provides the legal information on how we handle, process, and disclose personal information.

7.3 Employee Personal Data

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee or prospective employee personal information.

All employees are provided with our Staff Handbook which informs them of their rights under the data protection laws and how to exercise these rights.

7.4 The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 (collectively, The Rights of Data Subjects), in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. This is provided in our Privacy Notice.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity (i.e. verbally, electronic).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we cannot comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

7.4.1 Subject Access Request

Where a data subject asks us to confirm whether we hold and process personal data concerning them and requests access to such data; we provide them with:

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by the Company from the data subject, any available information as to the source and provider

Subject Access Requests are passed to the DPO as soon as received and a record of the request is noted. Subject Access Requests are always completed within 30 days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

7.5 Data Portability

The Company provides all personal information pertaining to the data subject to them on request and in a format that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used, and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

7.6 Rectification and Erasure

7.6.1 Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d), all data held and processed by the Company is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The DPO is notified of the data subjects request to update personal data and is responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, ensuring that all data relating to the subject is updated where incomplete or inaccurate.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

7.6.2 The Right to Erasure

In specific circumstances, data subjects have the right to request that their personal data is erased, however the Company recognise that this is not an absolute ‘right to be forgotten’. Data subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies:

- 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 collected or processed
- The personal data must be erased in order to comply with a legal obligation

Where one of the above conditions applies and the Company received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the DPO according to procedures outlined in this policy, to ensure that all data relating to that individual has been erased.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued storage and/or processing. While our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with, and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed:

1. The request is allocated to the DPO and recorded on the Erasure Request Register
2. The DPO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure as listed above
4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where the Company has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. Such refusals to erase data include:

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims
- If the data has been anonymised, collated, and shared (either with partner agencies or published publicly)

7.7 The Right to Restrict Processing

There are certain circumstances where the Company restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit. Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The Company will apply restrictions to data processing in the following circumstances:

- Where an individual contests the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- 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 we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as opposed to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise, or defend a legal claim

The DPO reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third parties. Where data is restricted, and we have disclosed such data to a third party, we will inform the third party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

7.8 Objections

Data subjects are informed of their right to object to processing in our Privacy Notice in a clear and legible form and separate from other information. Individuals have the right to object to:

- Processing of their personal information

Where the Company processes personal data for the performance of a legal task, in relation to our legitimate interests, or for research purposes, a data subjects' objection will only be considered where it is on 'grounds relating to their particular situation'. We reserve the right to continue processing such personal data where:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise, or defence of legal claims

Where a data subject objects to data processing on valid grounds, the Company will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

8. Oversight Procedures

8.1 Security Breach Management

Whilst every effort and measure are taken to reduce the risk of data breaches, the Company has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

The Company's 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.

The Data Breach Policy and Procedures outlines the specific policy and procedures to follow in the event of a data breach.

8.2 Information on Desks, Screens, and Printers

Members of staff who handle confidential paper documents should take the appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends, and at other unattended times.

Care should be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

8.3 Firewalls and Malware

The Company understands that adequate and effective firewalls, malware, and protected gateways are one of the main and first lines of defence against breaches via the internet and our networks.

We utilise configured firewalls and have anti-virus applications running on all computers, networks, and servers. The designated IT service provider and the DPO are responsible for ensuring all company computers have up-to-date and adequate firewalls and malware.

9. Transfers and Data Sharing

The Company takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within Ireland and EU are deemed less of a risk than a third country or an international organisation, due to the data protection laws covering the former and the strict regulations applicable to all EU Member States.

We have written and signed Data Sharing Agreements in place before any data sharing occurs. Various Service Level Agreements in place also govern the sharing of data.

10. Employee Training

Through our strong commitment and robust controls, we ensure that all staff understand, have access to, and can easily interpret the data protection laws requirements and its

principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role.

Our DPO is available to assist staff with their training and ongoing queries.

11. Penalties

The Company understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. We recognise that:

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (Chapter IX) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

12. Responsibilities

The Company has appointed a DPO whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management, and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

13. Review

This Policy will be reviewed biennially, or earlier as new information and/or legislation requires.