Sustainability Matters CLG T/A International Sustainable Finance Centre of Excellence

Data Protection Policy

Document Control	
Authorised by:	Stephen Nolan
Date:	September 2023
Review Date:	March 2024
Drafted by:	William McLoughlin BL, Argent Business Consultants
Document Version:	2.00 (Licenced)
Data Protection Officer Point of Contact	
Name:	Stephen Nolan
Contact Details:	stephen.nolan@isfcoe.org
Document Review History	
Previous Document:	1.00
Previous Version:	1.00
Amended (Y/N):	N

ARGENT BUSINESS CONSULTANTS

Index

Part 1: Policy

1.1 Policy Introduction

This is the data protection policy for Sustainability Matters CLG t/a International Sustainable Finance Centre of Excellence of The Black Church, St. Mary's Place, Dublin 7, D07 P4AX, [hereby referred to as 'us', 'we' or 'the firm'] and was drafted by Argent Business Consultants on foot of high-level data mapping, data processes and procedures provided.

This is the second policy document, version 2.00 replacing version 1.00, and is drafted in accordance with updates on the Data Protection Commission's practice directives and guidance notes and required procedures concerning the General Data Protection Regulation and Data Protection Act 2018 both of which came into force on the 25th of May 2018.

At time of drafting, the ePrivacy Regulation will replace the ePrivacy Directive 2002/58/EC at some unknown date within the next year. At this stage the impact it may have on this firm, as such, this policy needs to be reviewed when the ePrivacy Regulation come into force.

The Data Protection Commission have issued a guidance entitled *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing* regarding the processing of children's data, however, this firm does not market, advertise or target services to children, nor rely on children's consent for the processing of children's personal data.

At the latest, this Data Protection Policy needs to be reviewed by March 2024.

This data protection policy, and associated policies and procedures, including but not limited to, Privacy Policy, Cookie Policy, Data Processing Agreement, have been drafted by William McLoughlin BL of Argent Business Consultants (www.argentbusinessconsultants.ie) and used by licence.

1.2 Data Protection Principles

Article 5 of the General Data Protection Regulation (GDPR) specifies data protection principles that must be upheld every time personal data is processed. They are:

- Fair, lawful and transparent processing of data
- Purpose limitation principle (data processed for specific purposes, etc.)
- Data Minimisation (minimum processing of data)
- Accuracy
- Proper Data Retention Periods
- Data Security (integrity and confidentiality)
- Accountability

Part 2: Data Protection Principles of this policy specifies how this firm incorporates each principle into its procedures and policies.

1.3 Policy Statement

This firm is a ‘data controller’ as defined by General Data Protection Regulation and the Data Protection Act 2018 and endeavours to:

- Comply with the Data Protection Act 2018 and best practice.
- Comply with General Data Protection Regulation.
- Comply with the principles of data protection.
- Protect the privacy rights of individuals whose data we process.
- Ensure that any personal data in the possession of the organisation is kept safe and secure.
- Support employees and senior management to meet their legal responsibilities as set out under the principles of data protection.
- Respect individual’s rights, regardless of who they are.
- Implement best practice or instructional notices from the Data Protection Commission.
- Provide awareness, adequate training and support to all employees that process personal data.

1.4 Policy Objectives

The objectives of this Data Protection policy are to:

- Outline how we endeavour to comply with the Data Protection Act 2018 and General Data Protection Regulation.
- To provide good practice guidelines for employees and senior management.
- To reduce the risk of and protect against any breach of the Data Protection Act 2018 and General Data Protection Regulation.
- To be prepared to answer any queries or address any concerns by the Data Protection Commission should they arise.
- To ensure that individuals are able to access their personal data upon request.
- Provide guidance in the event of any breach of personal data.
- To help reduce our liability or anyone acting on behalf of us in the event of a data breach.

1.5 Policy Scope

This Data Protection Policy applies to all management, employees and any subcontractor who is engaged to process personal data on behalf of us regardless of whether their role or job description requires or specifies any processing of personal data.

An abridged version of this policy, in the form of a Privacy Policy (which is also known as a Data Protection Statement), will be made public on our website for anyone to access.

The purpose of the Privacy Policy, which is separate to this Data Protection Policy, is to inform all data subjects and the public at large how we may process their data.

The Privacy Policy is separate to our Cookie Policy that is also available on our website. The Cookie Policy deals with specific data protection concerns relating to the use of the website and any other electronic forms of interaction.

This Data Protection Policy is internal to this firm but may be made available to any relevant third party upon request as part of entering into or complying with any data processing agreement between us and any relevant third party.

For the avoidance of doubt, if any party is seeking this Data Protection Policy, please refer them to the point of contact for data protection (please see ***Part 3.6: Data Protection Officer / Compliance Officer*** of this document).

1.6 Descriptions/Definitions

'Access Request' or 'Subject Access Request' is where an individual makes a request to an organisation for a copy of their personal data under Article 15 of the General Data Protection Regulation.

'Data' is any information that can be processed and includes automated data, manual data and electronic data.

'Data Controller' or 'controller; means a person, company or organisation who, either alone or with others, controls the contents and use of personal data. In a general context for the purposes of this policy, 'data controller' or 'controller' refers to this firm.

'Data Processing' is the performance of any operation in connection with the use of data, including:

- Obtaining, recording or storing data,
- Collecting, organising, altering or amending data,
- Retrieving or using data,
- Disclosing the data via transmission, dissemination, or the use of any method of communication or otherwise making the data available, and,
- Aligning, combining, blocking access to, erasing or destroying the data.

'Data Processor' or 'processor' means a person, company, organisation or any legal entity who processes personal data on behalf of a data controller. However, this does not include an employee of a data controller who processes personal data in the course of their employment (i.e. they are not considered a data processor for their employer).

However, a subcontractor of ours is considered a data processor in their own right and they are responsible for their own GDPR compliance subject to a data processing agreement (discussed later).

'Data Subject' means an individual who is the subject of Personal Data, i.e. they are identified by the data (e.g. name, address, phone number, etc.) and their data has been processed by someone.

'Personal Data' is any information that relates to an **identified or identifiable living individual**. Different pieces of information on their own might not be personal data but when collected together may lead to the identification of a particular person is also classed as personal data.

Examples of personal data (i.e. data that can identify a person) are:

- A name and surname
- A home address
- An email address such as **name.surname**@company.com or **surname**@company.com (but a general email addresses such as info@company.com is not personal data as it does not identify a person)
- A State issued identification card number (e.g. Public Service Card number, Passport Number, Driver's licence, etc.)
- Location data (e.g. location data on a mobile phone, tablet, etc.)
- An Internet Protocol (IP) address
- A cookie ID
- The advertising identifier (IDFA) on a mobile phone or device (i.e. a unique code that identifies the device and any user, etc.)
- Photos, recorded phone calls or video footage.
- Any data that, if used with other data, can identify a person.

Personal data that has be 'de-identified', encrypted or pseudonymised but can be changed back or decrypted to re-identify a person is still classed as personal data (i.e. if it can be unencrypted, changed or modified to identify a particular person).

Personal data that has been rendered anonymous in such a way that a person is not identifiable is not personal data but only **if the anonymisation is irreversible** (i.e. if you can't change the data back to personal data).

'Special categories of Personal Data' are personal data that relates to:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics
- Health
- Sex life or sexual orientation

The processing of special categories of personal data is generally prohibited except under certain conditions but in general:

- The data subject has made one or more of the special categories of personal data manifestly public (but the condition only applies to what data was made public),
- The data subject has given **explicit consent,**
- A law permits and governs the specific type of data processing for a specific purpose related to public interest or health (e.g. Mental Health Acts),
- A law that permits processing includes adequate safeguards and provides for the processing of sensitive personal data in areas such as public health, employment and social protection (e.g. notifying Revenue of PAYE returns, etc.).

Please see ***Part 2: Data Protection Principles*** for the full conditions required for the processing of special categories of personal data.

There are two main pieces of legislation that combined deal with the majority of all data protection matters in Ireland; the EU General Data Protection Regulation and the Irish Data Protection Act 2018.

Part 2: Data Protection Principles

2.1 Introduction

Article 5.1 of the General Data Protection Regulation (EU 2016/679) mandates compliance with the following Data Protection Principles.

1. Fair, lawful and transparent processing of data
2. Purpose limitation principle
3. Data Minimisation
4. Accuracy
5. Proper Data Retention Periods
6. Data Security
7. Accountability

Which in turn gives data subjects the following rights:

1. Right to be informed of processing of personal data
2. Right of access to their personal data
3. Right of rectification of their personal data
4. Right of erasure of their personal data
5. Right to restrict processing of their personal data
6. Right to data portability of their personal data
7. Right to object to processing of their personal data
8. Rights relating to automated decision making and profiling

The above principles are used as a basis for the creation of this policy from Part 2 onwards. Whereas from the Rights of Data Subjects are reflected in our practices on how we deal with personal data and data subjects from Part 3 onwards.

We recognise that our people have legal responsibilities relating to the processing of personal data and this policy is to help ensure our people protect themselves from any breaches of the Data Protection Act 2018 and GDPR requirements and in doing so, uphold and protect individuals' privacy rights.

We incorporate and apply the data protection principles as expanded upon in the following sections, insofar as possible, into all commercial and working practices, thereby reducing the risk of any data breach.

We will only process the minimum amount of personal data that is necessary to achieve our purpose(s). In order to achieve this, Privacy Impact Assessments may be conducted for new processes and procedures to help reduce any data protection concerns and ensure the data protection principles are incorporated into our work.

For existing, and or ongoing, processes and procedures, information sought from data subjects must be:

- Adequate for the purpose(s) for which it is sought (i.e. required to fulfil the purpose);
- Relevant to the purpose(s) for which it was sought;
- Not excessive in relation to the purpose(s) for which it was sought.

There should be periodic reviews of the relevance of personal data sought from data subject through various channels (e.g. through our website, order forms, etc.) and periodic reviews as to the basis for collecting or storing any information, to ensure ongoing compliance.

2.2 Fair, lawful and transparent processing of data

To fairly obtain data a data subject must, at the time of the personal data being collected, be made aware of:

a) The name of the data controller (which in this case is this firm);
b) The name of any data processor used by the data controller;
c) The purpose(s) of collecting the data;
d) The identity of any representative nominated for the purpose of the Acts (i.e. any Data Protection Officer or point of contact for data protection enquiries, etc.);
e) Whether replies to questions asked are obligatory and the consequences of not providing replies to those questions (e.g. mandatory fields in order forms);
f) The existence of the right to access by a data subject to their personal data;
g) The right to rectify the data subject's personal data if inaccurate or processed unfairly;
h) The right of erasure, to have irrelevant data removed, destroyed or deleted after a reasonable amount of time (i.e. subject to a fair data retention policy)
i) Any lawful grounds of a third party accessing or processing the data subject's personal data (e.g. mandatory reporting in accordance with a child protection policy, criminal offences, etc.)
j) Any other information which is necessary so that processing may be considered fair;
k) Any information necessary to make the data subject aware as to the extent that their personal data will be processed;
l) In circumstances where the personal data is not obtained from the data subject (e.g. via a third party) then the above information must be provided to the data subject and they must be informed as to the identity of the original data controller from whom the information was obtained (i.e. where the personal data came from) and the categories of data concerned (i.e. what personal data was given).

There must be a **lawful basis for processing data** and there are differences between lawfully processing personal data and lawfully processing special categories of personal data.

In order to **lawfully process personal data**, you need **at least one** of the following grounds:

- ***Consent*** from the data subject (clear and unambiguous consent).

- ***A legitimate interest*** – this means the processing of data is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the individual. In practice, this may be difficult to rely upon as the ground of processing depends on the set of circumstances and whether those circumstances justify processing personal data.

For example, GDPR permits disclosing personal data to An Garda Síochána in order to stop immediate harm and or a serious criminal offence from being committed, thereby ensuring the health, safety and wellbeing of a person.

- ***Necessary for the performance of a contract***. When a data subject willingly enters into a contract it may not be possible to perform that contract without processing their personal data, e.g. a contract for the purchase of a newspaper subscription - you need the name and address of the data subject in order to deliver the newspaper. In other words, if you do not process the data subject's personal data then the contract cannot be performed or fulfilled.

- ***Legal obligation.*** The processing is necessary for compliance with a legal obligation on the part of the data controller e.g. mandatory reporting of child protection concerns under the Children First Act 2015.

- ***Vital Interests.*** That the processing is necessary to protect the vital interest of the individual or of another natural person. Again, this is a difficult condition to rely on but, again, an extreme example would be disclosing personal data to An Garda Síochána in order to negate an immediate threat of danger against a person.

- ***Public Functions.*** The processing may be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

In order to **lawfully process special categories of personal data** you need **at least one** of the following grounds:

- ***Explicit consent*** (clear and unambiguous explicit consent)

- ***Legal obligation related to employment*** - this requires the organisation to fulfil legal requirements related to employment, e.g. provide PAYE details under the Revenue Acts, provide certain details to Social Welfare (PRSI contributions, etc.).

- ***Vital interests***. This is where the processing is necessary to protect the vital interest of the individual or another person where the data subject is legally or physically unable to provide consent.

- ***Not-for-Profit bodies***. This category specifies that the process may be carried out for the legitimate activities, with appropriate safeguards, of a not-for-profit body (e.g. a charity) on the condition that the processing only relates to members or related persons, including former members, or people who have regular contact with the organisation in connection with its purpose (may include volunteers) and the personal data is not disclosed outside that organisation without consent.

- ***Public information.*** Where the processing relates to special categories of personal data that was manifestly made public by the individual (limited to the category or categories made public by the individual and not other categories).

- ***Legal claims.*** This relates to the procession of personal data necessary for the establishment, exercise or defence of legal claims of being processed by courts acting in their judicial capacity.

- ***Substantial public interest or public health.*** Where processing is necessary for reasons of substantial public interest and or public health. In practice, this may be a very difficult ground for a private organisation to rely on.

- ***Healthcare***. The processing is necessary for the purposes of preventative or occupational healthcare, or for assessing the working capacity of an employee, medical diagnoses related to occupational workplace capacity (e.g. workplace health assessments, employer medical assessments, etc.) and or the procession of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Irish law or pursuant to a contact with a health processional and is subject to suitable safeguards.

- ***Archiving.*** The processing is necessary for archiving scientific or historical research purposes or statistical purposes.

If at any stage an employee or management are unsure as to any lawful ground of processing personal data or special categories of personal data, please refer the matter to the organisation's point of contact for data protection as a matter of urgency. Please see ***Part 3.6: Data Protection Officer / Compliance Officer*** for further information.

Note: *For the avoidance of any doubt, if you are about to process someone's personal data and you are not sure as to why you are doing it, whether it is necessary or the lawful basis for processing the data then stop, do not process any data until you have discussed the matter with your organisation's point of contact for data protection.*

2.2.1. Data belonging to Children

Under GDPR, the default age at which a person is no longer considered a child for the purposes of consent is 16 but GDPR allows EU Member States to adjust that limit to anywhere between 13 to 16. The Irish position is 16 years of age for digital consent under the Data Protection Act 2018. This digital age of consent, and issues as to how this works in practice, will be subject to review by the Minister for Justice who will issue ongoing directives and guidance on same.

In cases where services are specifically provided to persons under 18 (ages 16 & 17) then data controllers must ensure privacy notices or data protection statements are written in a clear, plain manner in such a language that they would understand.

In cases of processing a child's personal data, and where consent is relied upon as a basis for the lawful processing of their data, then consent must be given or authorised by a person with legal responsibility for the child (e.g. parent, guardian, etc.).

At time of drafting, the Data Protection Commission have published *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing* with 14 key principles for processing children's personal data, which are as follows[1]:

1. **Floor of protection:** Online service providers should provide a "floor" of protection for all users, unless they take a risk-based approach to verifying the age of their users so that the protections set out in the Fundamentals are applied to all processing of children's data.

2. **Clear-cut consent:** Where a child gives consent to the processing of their data, that consent must be freely-given, specific, informed and unambiguous, made by way of a clear statement or affirmative action.

3. **Zero interference:** If you are relying on legitimate interest(s) as a lawful basis for processing children's personal data, you need to ensure that these legitimate interests do not interfere with, conflict with or negatively impact, **<u>at any level</u>**, the best interests of the child.

4. **Know your audience:** Online service providers should take steps to identify their users and ensure that services directed at, intended for or likely to be accessed by children have child-specific data protection measures in place.

[1] https://www.dataprotection.ie/en/dpc-guidance/blogs/the-children-fundamentals

5. **Information in every instance:** Children are entitled to receive information about the processing of their own personal data irrespective of the legal basis relied on. This is even the case where consent was given by a parent on their behalf to the processing of their personal data.

6. **Child-oriented transparency:** Privacy information about how personal data is used must be provided in a concise, transparent, intelligible and accessible way, using clear and plain language that is easy to understand and suited to the age of the child.

7. **Let children have their say:** Remember that children are data subjects in their own right and have rights in relation to their personal data at any age. As such, the DPC considers they should be allowed to exercise their data protection rights at any age so long as they have the capacity to do so and it is in their best interests.

8. **Consent doesn't change childhood:** Just because you have valid consent from a child or their parent/guardian doesn't mean you can treat the child like an adult. You still need to provide the specific protection that children merit under the GDPR.

9. **Your platform, your responsibility:** Companies who derive revenue from providing or selling services through digital and online technologies pose particular risks to the rights and freedoms of children. Where such a company uses age verification and/ or relies on parental consent for processing, the DPC will expect it to go the extra mile in proving that its measures around age verification and verification of parental consent are effective.

10. **Don't shut out child users or downgrade their experience:** If your service is directed at, intended for, or likely to be accessed by children, you can't bypass your obligations simply by shutting them out or depriving them of a rich service experience.

11. **Minimum user ages aren't an excuse:** You can't absolve yourself of your controller responsibilities to child users by simply stating that children below a certain age aren't welcome on your platform/service. If your service isn't intended for children under a certain age, then you need to take steps to ensure that your age verification mechanisms are effective at preventing children below that age from accessing your service. If this is not a viable option, then you need to ensure that appropriate data protection measures are in place to safeguard the position of child users, both below and above the official user age threshold.

12. **Prohibition on profiling:** Don't profile children for marketing or advertising purposes unless you can clearly show how and why it is in their best interests to do so.

13. **Do a DPIA:** You should do Data Protection Impact Assessment for all processing of children's personal data given their particularly vulnerability. The best interests of the child must be a key consideration in any DPIA and should outweigh your commercial interests or those of a third party.

14. **Bake it in:** Online service providers that routinely process children's personal data should, by design and by default, have a consistently high level of data protection which is "baked in" across their services

We do not target of profile children nor do we routinely process personal data belonging to children.

2.2.2. Data belonging to Vulnerable Adults

We do not target of profile vulnerable adults nor do we routinely process personal data belonging to vulnerable adults.

2.2.3. Consent for CCTV (including webcams & dashcams)

Reasonable use of CCTV for certain uses is permitted but subject to a CCTV policy that ensures data subjects are still afforded the protections of the GDPR and Data Protection Acts.

We do not use any CCTV or cameras in our offices.

There are circumstances where video footage may be processed without the consent of data subjects but there has to be a lawful ground of processing which depends on the context and particular circumstances of each ground (footage use, why it's retained, etc.).

We use webcams, voice over internet (VoIP) and teleconferencing when engaged with employees, subcontractors and, on occasions, clients or potential clients.

Please see ***Schedule 1*** - ***Annex 1 – Use of CCTV, webcams and dashcams*** for the organisation's position on the use of CCTV, webcams and dash cams.

Please refer to our employee handbook for our firm's position on the use of social media.

2.3 Purpose limitation principle

Personal data processed must be processed for a specific purpose, especially if consent is relied upon as a lawful ground of processing. If personal data is used for another purpose, then it invalidates consent. However, if consent is invalidated, the organisation may be able to rely on an alternative lawful basis of processing.

Any data subject has the right to question the purpose for which their data is being held and the organisation must be able to identify that purpose when requested.

In order to comply with this requirement, management, employees and sub-contractors should be aware:-

- that a person is entitled to know the specific reasons why their data is being processed;
- the lawful basis for processing personal data;
- of the different categories of data which are held; and,
- any specific lawful basis for processing each category of special categories of personal data.

All employees should be able to identify the above information as necessary; however, the organisation has appointed a single point of contact for all data protection matters. Please see ***Part 4.2: Data Access Request*** for full information on a data access request including what to do if you get a data access request.

Employees are not to disclose any personal data to any third party without the explicit consent of the data subject; ideally recorded in writing by way of email or letter from the data subject unless there is a lawful exemption to this depending on the circumstances (e.g. in case of emergency to prevent injury, prevent a crime, to contact police, etc.)

Personal data about data subjects should not be disclosed to colleagues unless the data is required to fulfil authorised duties or work, or there is a lawful exception as identified by our firm or our firm's point of contact for data protection matters.

Sub-contractors will be bound by an appropriate data processing agreement (discussed later).

2.4 Data Minimisation

The Data Protection Act 2018 and GDPR place the onus on a data controller (and a data processer) to process the minimum amount of personal data required in order to complete the data controller's objective.

In other words, if we request personal data from someone then the request must be relevant to what we want to do with the data. We can only request the minimum amount of data required to fulfil any lawful purpose we identify.

For example, if somebody voluntarily signed up to a marketing campaign then their name, address, email address and phone number might be required. Any further data requested may be excessive (e.g. their medical records, family status, etc.) and may be in breach of the Data Minimisation principle under GDPR.

The same principle applies when a data controller engages a data processer to process data on their behalf. The data controller can only provide the minimum amount of relevant data necessary for the data processer to complete their tasks. Anything beyond the minimum amount necessary is excessive and may be in breach of GDPR.

We are committed to only processing the minimum amount of data required to achieve its goals.

2.5 Accuracy

We endeavour to support all employees and management, and any relevant third parties where we may act as a data processor, by maintaining records of personal information that are accurate, complete and up-to-date. Apart from being requirements of data protection legislation, it is in our interest to ensure data is accurate for reasons of efficiency and effective decision making.

As such, it is important to note that:

- Manual and computer procedures are suitable to maintain high levels of data accuracy;
- Managerial departments or divisions should have regular review cycles or procedures to ensure information processed is accurate and up-to-date;
- Management ensure periodical reviews and auditing of procedures to ensure data processed is accurate and up-to-date; and,

- Where a data subject advises of any changes to their personal data, or any mistakes in their personal data, that the personal data is amended or destroyed as soon as possible.

Data subjects have the right to ensure their personal data being processed is accurate. They are also entitled to ask any entity (i.e. any data controller or data processor) whether they have any personal data relating to the data subject. If so, the data subject is entitled to get copies of that data and demand any inaccurate data be corrected (or even deleted or destroyed in certain cases).

For more information, processes and how do deal with inaccurate personal data, please see ***Part 4: Rights of Data Subjects.***

Please note in cases where personal data is found to be inaccurate and rectified, there may be a requirement to retain the 'old incorrect data' for auditing or compliance purposes.

Another example would be where a bank charges an incorrect interest rate on a mortgage. When the mistake is discovered, it cannot be deleted and replaced with the correct interest rate as this would contradict previous bank statements. The mistake must be recorded on the record, i.e. in a transparent manner, to explain any differences in calculations, etc. and how the bank arrived at the final outstanding amount due.

Any employee who discovers a mistake in personal data or is notified of a mistake in personal data by a data subject, is to liaise with the organisation's point of contact on data protection in order to best address, delete, alter or correct the personal data, as appropriate under the circumstances.

2.6 Proper Data Retention Periods

Personal data should only be retained for the time necessary for the purpose(s) of which it was processed. As soon as personal data is no longer necessary, it should be destroyed or deleted in an appropriate manner, subject to the following retention period.

The following is an edited overview of the company's data retention policy. For the full policy please see ***Part 3.5: Data Retention Policy***.

We have a general personal data retention period of **seven years** from the last interaction with a client or attendee at an event we organise (or seven years from the last contractual relationship with a client or attendee at an event). The figure of seven years is arrived at following legal advice and is based on six years for the statute of limitations for breach of contract (but there are some exceptions) plus one year to serve a summons, equating to seven years in total.

Exceptions to the above limitation period may include:

- Tax record and payroll records for taxation purposes that are subject to Revenue retention periods;
- Employment interviews and data relating to interview and selection of potential employees (e.g. CVs, cover letters, etc.) of which data relating to unsuccessful candidates will be retained for **one year** after the closing of the relevant selection period, or job interviewed, to allow service relating to any matter that may arise relating to the selection or employment process (e.g. any complaint relating to employment under the Employment Equality Acts);
- Data that may assist in the reporting, investigation or litigation relating to a criminal offence that may reasonably affect the organisation;
- Any personal data that the organisation deems appropriate under the circumstances to retain outside the standard eight year retention period, subject to the requirement to document the reasons why the personal data is being held and incorporating regular reviews as to the necessity of retaining such data that will be destroyed or deleted once no longer required;
- Data relation to accidents or 'near misses' that require a mandated investigation under Health, Safety and Welfare at Work legislation.

2.7 Data Security

Appropriate security measures must be taken again unauthorised access to, or alteration, disclosure, sharing or destruction of personal data; this includes protecting against any accidental loss, dissemination or destruction of data.

To protect personal data, our security includes the following practices and procedures;

- Access to any personal data within the organisation is restricted to authorised people for legitimate purposes only;
- Access to computer systems is password protected;
- Non-disclosure of personal security passwords to any individual (including other employees or contractors);
- Information on computer screens and manual files are kept out of sight from callers or visitors to our premises;
- Paper based data are securely held in locked cabinets, locked rooms and rooms with limited access with the only access restricted to people who have a legitimate use for the secured data;
- Special care, including encryption, must be taken regarding the use, access, location and storage of any mobile computing device and storage devices, e.g. laptops, USB drives, etc. and all mobile phones and laptops are password protected;
- Personal data is not stored on portable devices except in essential circumstances for short time use, for as briefly as possible. Where deemed essential, the data must be encrypted and deleted from the portable device as quickly as possible. Personal data is not to be stored long term in any removable, easy to use USB sticks or flashcards;
- All reasonable measures are to be taken to ensure all employees are made aware of all security measures in order to comply with them;
- Any physical paper that contains personal data that is no longer necessary to be retained must be destroyed as soon as possible via appropriate shredding techniques using a suitable shredder (e.g. cross-cutting shredding).

The Data Protection Commission advises whole-disk encryption of 256-bit strength should meet the present requirements and further advises that a strong password would typically be 14 characters long, contain a random selection of letters, numbers and symbols and be impossible to guess[2].

[2] https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190625%20Data%20Security%20Guidance.pdf June 2019 Guidelines

2.8 Accountability

We endeavour to comply with the General Data Protection Regulation, the Data Protection Act 2018 and data protection best practices. This Data Protection Policy states our data protection objectives and standards we wish to maintain.

This policy will be made available internally within the organisation to all employees and in some cases to third parties acting as our agent and or data processor on a case-by-case basis (or further data processors as the case may be), so everyone working with or on behalf of us understands our commitment to data protection. This also shows our commitment to transparency to employees and stakeholders as part of good governance.

This policy may also be made available to any data controller to whom we may act as a data processor and process personal data on their behalf. This policy can be used to show compliance with GDPR and Data Protection Act 2018 as part of any data controller/processor relationship.

In terms of transparency and accountability to our clients, data subjects and the public at large, we publish an abridged version of this Data Protection Policy, in the form of a Privacy Policy (which is also referred to as a Data Protection Statement), on our website for anyone to examine. We are also upfront and transparent with how our website users' data will be used/processed via our Cookie Policy that is also available on our website.

As part of the Privacy Policy online, we explicitly tell data subjects and the public at large how their data (if they chose to provide it) will be used. We also explain how we process personal data for our marketing and advertising purposes which allows people to decide whether they want to 'opt in' to our marketing and advertising communications, etc.

Marketing & Advertising

At the time of drafting this policy, we do not engage in targeted advertising to specific data subjects. However, if we do decide to do so, then we will only process personal data for commercial marketing and targeted advertising with the explicit consent of data subjects and in accordance with our Privacy Policy.

In such an event, we will process data that originates directly from a data subject for marketing or advertising purposes and has been voluntarily provided to us (i.e. the lawful basis for processing is consent).

When we process personal data for marketing or advertising purposes we do so on the basis of consent provided by a data subject. Clients, users, data subjects and members of the public do not have to sign up or ‘opt in’ to our marketing or advertising activities to use our website or to find out information about our organisation yet they may choose to do so subject to our Privacy Policy (with specific regard to the marketing and advertising section of the Privacy Policy) that is available on our website. We do not engage in any ‘pre-ticked’ boxes for consent nor do we automatically require someone to ‘opt out’ of any marketing or advertising communications.

Any person (or data subject) is entitled to withdraw consent to any marketing or advertising purposes at any stage. To facilitate this, we provide an option for people to ‘unsubscribe’ or not to be contacted again as part of any direct or targeted marketing or advertising communications.

We respect a person’s decision to withdraw their consent and will act upon it immediately without pressing them for reasons as to why they seek to withdraw consent.

Part 3: Risk Management & Compliance Audits

3.1 Internal Compliance

We endeavour to protect the privacy of all data subjects; including employees, clients, third party contractors/suppliers and the public at large.

We do this by appointing a single point of contact within the organisation for all data protection related matters. The single point of contact is identified on the cover of this document.

This document replaces any previous data protection policy that will be kept on file for auditing purposes.

At the time of drafting, guidance notes or practice directives issued by the Data Protection Commission have been incorporated into this policy but the Data Protection Commission has indicated that further guidelines and directives may be published at later dates. Any such future instructions must be incorporated into this document as part of the next review.

At time of drafting, the ePrivacy Regulation is due to come into force at some unspecified future date. As such, this document needs to be reviewed in preparation for same when the final text of the ePrivacy Regulation is published.

Data Protection Policy - Document control

This document is Version 2.00 and replaces the previous policy document (version 1.00). At the latest, this policy document must be reviewed by March 2024.

3.2 External Compliance

We may be subjected to any enquiry or audit by the Data Protection Commission.

Any enquiry from the Data Protection Commission is to be referred to our internal point of contact for all data protection matters whose contact details are on the front of this policy.

All management, employees, sub-contractors and or data processors are required to fully cooperate with any audit by the Data Protection Commission; failure to do so may, under the circumstances, and in an employee's case, be the basis for initiating our grievance and disciplinary procedure. Furthermore, such a failure to cooperate may under the circumstances be considered gross misconduct due to the severity of non-cooperation and or possible outcome to the organisation, employee, client or data subject involved.

In terms of a sub-contractor or data processors, the failure to engage with any data audit or request to show compliance with GDPR or the Data Protection Act 2018 as required will be a basis for discontinuation of services and possible legal action.

We may, at our sole discretion, appoint an external auditor to periodically assess and review internal data protection policies and practices. In such cases, all employees are expected to fully cooperate with any such appointed auditor.

We may also appoint an external consultant to assess or advise on any data breaches or potential data breaches. In such cases, all employees are expected to fully cooperate with any appointed investigator.

We may outsource one or more of our data protection role and responsibilities. In such an event, we are still considered a data controller under GDPR and the Data Protection Act 2018 and an appropriate data processing agreement, between us and any relevant data processer, shall be put in place.

3.3 Privacy Impact Assessments (PIA)

A Privacy Impact Assessment (PIA), which can also be referred to as a Data Protection Impact Assessment (DPIA), is a risk assessment tool introduced under Article 35 of the General Data Protection Regulation (GDPR) and is used to ensure the ongoing privacy rights of all data subjects are upheld.

A PIA is a process designed to describe the processing, assess the necessity and proportionality of any processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them).

PIAs are important tools for accountability as they help data controllers not only to comply with requirements of the GDPR and Data Protection Act 2018 but also to demonstrate that appropriate measures have been taken to ensure compliance. If implemented correctly, PIAs may help reduce liability in the event of an actual breach occurring.

In essence, a Privacy Impact Assessment is required for any new or contemplated data processing activity where the processing is, as per Article 35(1), "*likely to result in a high risk to the rights and freedoms of natural persons*".

Generally speaking, if the processing of data is unlikely to result in any risk to personal data or privacy rights then a PIA is not required.

In November 2018, the Data Protection Commission issued guidance on when a PIA is required.[3]

In short, and using simple terms insofar as possible given the wording used by the Data Protection Commission, a PIA is mandatory in cases were:

1. Use of personal data on a large-scale for a purpose(s) other than that for which it was initially collected.
2. Profiling vulnerable persons including children to target marketing or online services at such persons.
3. Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects.
4. Systematically monitoring, tracking or observing individuals' location or behaviour.
5. Profiling individuals on a large-scale.

[3] https://www.dataprotection.ie/en/guidance-landing/data-processing-operations-require-data-protection-impact-assessment

6. Processing biometric data to uniquely identify an individual or individuals or enable or allow the identification or authentication of an individual or individuals (subject to further requirements set out by the Data Protection Commissioner).
7. Processing genetic data in combination with any of the other criteria set out by the Data Protection Commission.
8. Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort. Note this may include using personal data that originated from another source (e.g. buying a mailing list, using someone else's customer lists, etc.)
9. Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources where processing was/is carried out for difference purposes or by different controllers.
10. Large scale processing of personal data where the Data Protection Act 2018 requires "suitable and specific measures" to be taken in order to safeguard the fundamental rights and freedoms of individuals.

This is a very complicated area of GDPR and the Data Protection Commission has attempted to simplify it by stating where a PIA is not required, however, for the purposes of our data processing practices, and notwithstanding the above list, a PIA is **not required** where:

- Processing operations (or processing the personal data) do not result in a high risk to the rights and freedoms of individuals.
- Where processing was previously found not to be at risk by PIA (i.e. a PIA was previously done then there is no need to do it again for the same processing of personal data).
- Processing has been authorised by the Data Protection Commissioner (who issues numerous guidance notes and directives on their website www.dataprotection.ie).

We are required to consider whether a PIA is required on a case-by-case basis for any data processing or service offered, or any change in existing processes or services that currently processes personal data (including contact details). This requirement includes any instance in which the organisation may expand into new products or services that may impact on any current processing arrangements.

The reason for assessing the need of a PIA on a case-by-case basis is so we are aware of any potential risk or threat to personal data and can show that the risk or threat was considered and assessed appropriately. A PIA creates an audit trail to show we are compliant with data protection practices and risk and governance best practices.

“***likely to result in a high risk to the rights and freedoms of natural persons***”**.**

In addition to the above, the Article 29 Working Party (an EU body set up to interpret GDPR) issued *Guidelines on Data Protection Impact Assessment (DIPA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*[4] which is incorporated into our privacy impact assessments.

We have a screening questionnaire in ***Schedule 2 – Annex 1*** to assist in deciding on a whether a PIA is required, however, this is provided as an indicator and not a definitive assessment tool.

If anyone is unsure whether a PIA is required, best practice would be to complete a PIA in order to reduce any risk to data subjects..

For details of all the processes involved and requirements of a PIA please see ***Schedule 2*.**

All employees and contractors are to liaise with the organisation’s point of contact for data protection on any matter relating to a PIA who will in turn, sign off on any completed PIA.

[4] https://ec.europa.eu/newsroom/article29/items/611236

3.4 Data Protection by Design and Default

GDPR and the Data Protection Act 2018 enshrine both the principle of ‘privacy by design’ and the principle of ‘privacy by default’ into law. This means that any product or service settings must be automatically privacy friendly and requires the development of services and products to take account privacy considerations from the outset.

In short, when we are considering any new service or process, we must enshrine data subjects’ privacy throughout the entire process (privacy by design) and then must further ensure that default settings ensure privacy, e.g. boxes to consent to marketing cannot be pre-ticked, data subjects must opt-in instead of opting out, etc. (privacy by default).

The firm’s point of contact for all data protection matters must be consulted on any new services, products or procedures to ensure privacy by design and privacy by default are incorporated into the design, testing and rollout or implementation phases.

Failure to implement data protection by design or data protection by default can be an offence under GDPR and or the Data Protection Act 2018.

3.5 Data Retention Policy

Personal data should only be retained for the time necessary for the purpose(s) of which it was processed. As soon as personal data is no longer necessary, it should be destroyed or deleted in an appropriate manner, subject to the following retention period.

We have a general personal data retention period of **seven years** from the last interaction with a client or attendee at an event we organise (or seven years from the last contractual relationship with a client or attendee at an event).

The figure of seven years is arrived at following legal advice and is based on six years for the statute of limitations for breach of contract plus one year to serve a summons, equating to seven years in total.

In other words, we retain personal data for seven years so we can defend against any legal claim from a data subject (and our lawful basis to process the personal data is to protect against legal claims and Article 6.1(a), Article 6.1(c), Article 6.1(f) of GDPR). After seven years any legal claim a data subject may have against us is statue barred and they cannot sue us.

Our general data retention period of seven years has the following exceptions:

- Tax record and payroll records for taxation purposes that are subject to Revenue retention periods;

- Employment interviews and data relating to interview and selection of potential employees (e.g. CVs, cover letters, etc.) of which data relating to unsuccessful candidates will be retained for one year after the closing of the relevant selection period, or job interviewed, to allow service relating to any matter that may arise relating to the selection or employment process (e.g. access to employment under the Employment Equality Acts);

- Data that may assist in the reporting, investigation or litigation relating to a criminal offence that may reasonably affect the organisation.

- Any data that needs to be retained in order to protect against, or for the purposes of, any future or ongoing litigation (e.g. if there is ongoing litigation by a data subject then we are entitled to keep/process the data until the trial of the case is over, etc.).

- Any data which we deem appropriate under the circumstances to retain outside of the standard seven year retention period, subject to regular reviews as to the necessity of retaining such data that will be destroyed once no longer required.

- Any data retained under specific legislative provisions (e.g. CRO data on directors under the Companies Acts).

- Data relating to relevant accidents in the workplace (not just affecting employees) will be held for **ten years**:

  The Safety, Health and Welfare at Work (General Application) Regulations 2007 (S.I. No. 299 of 2007) mandates the organisation **must** report and investigate certain accidents, or 'near misses', in the workplace.

  As part of this investigation process, the organisation must retain certain information relating to an accident, e.g. parties involved, causes, investigation, outcome, CCTV footage (if available) for a period of **ten years**.

  Section 226 of The Safety, Health and Welfare at Work (General Application) Regulations 2007 (S.I. No. 299 of 2007) as, inserted by Section 6 of Safety, Health and Welfare at Work (General Application) (Amendment)(No. 3) Regulations 2016 (S.I. No. 370 of 2016), specifically states a mandatory ten year period to retain records relating to a relevant accident.

The table below is a non-definitive indicative guideline for reference use and is not to be relied upon without independent legal advice.

Note: Data related to any ongoing legal and investigative actions should **not** be destroyed but identified and stored safely until no longer necessary.

Documents	Retention Period	Legal Basis for retention/processing
Finance		
If applicable, Ledgers/Journals	7 years since client left	S. 886 Tax Consolidation Act 1997
If applicable, banking documents, payment records, etc.	7 years since client left	S. 903 & 1064 Tax Consolidation Act 1997

If applicable, client budgets, financial forecasts, etc.	7 years since client left	
If applicable, details of any client Assets, Capital property, etc.	7 years since client left	S. 886 Tax Consolidation Act 1997
If applicable, debts, collections, bad debts, etc.	7 years since client left or until any legal action is resolved (See Legal below)	S. 886 Tax Consolidation Act 1997 S. 11.4 Stature of Limitations Act 1957
Revenue		
Income Tax	10 years	S. 886 & s. 1064 Tax Consolidation Act 1997
Corporation Tax	10 years	S. 886 & s. 1064 Tax Consolidation Act 1997
Capital Gains Tax	10 years	S. 886 & s. 1064 Tax Consolidation Act 1997
VAT	6 years	Value Added Tax Consolidation Act 2010
Employment		
Employment Contract	7 years after employee left	s. 25 Organisational of Working Time Act 1997 S.I. 473 of 2001 s. 11 Statute of Limitations 1957
Employee Terms or Benefit plans (insurance, pensions, etc.)	7 years after employee left	S. 886 & s. 903 Tax Consolidation Act 1997 s. 11 Statute of Limitations 1957
Employment interviews	If the applicant was successful then up to 7 years after employee left. If the applicant was unsuccessful then 12 months after the interview	As above. S.8 & s. 77 Employment Equality Act 1998.
Employee files / evaluation records	7 years after employee left	s. 25 Organisational of Working Time Act 1997 S.I. 473 of 2001

		s. 11 Statute of Limitations 1957
Employee Investigations / Disciplinary matters	7 years unless there is ongoing legal action then can be retained until no longer necessary (see Legal below)	
Holiday leave	7 years after employee left	
Parental leave & Force Majeure leave	8 years or 7 years after employee left (whichever is longer)	s. 27 Parental Leave Acts
Carer's Leave	8 years or 7 years after employee left (whichever is longer)	s. 31 Carer's Leave Act 2001
Accident in the workplace	7 years unless the accident is a "notifiable accident" or "dangerous occurrence" to the Health & Safety Authority **If "notifiable accident" or "dangerous occurrence" then 10 years** **If unsure of the type of accident, check with the Health & Safety Authority**	s. 6 Safety, Health and Welfare at Work Regulations 2016 (SI No 370 of 2016)
Health & Safety		
Any Accident	7 years unless the accident is a "notifiable accident" or "dangerous occurrence" to the Health & Safety Authority	s. 6 Safety, Health and Welfare at Work Regulations 2016 (SI No 370 of 2016)
Legal		
Where there is no legal action	7 years (Statute barred after 6 years + 1 for service) **If unsure seek expert advice**	s. 11 Statute of Limitations 1957
Where there is legal action	Keep until no longer necessary **If unsure seek expert advice**	

CCTV		
CCTV / Webcam / Dashcam footage	4-6 weeks unless: 1. Relates to an investigation (see above) 2. Relates to an accident (see above) 3. Relates to legal action (see above) **If unsure seek expert advice**	

Care should be taken to ensure that data are disposed of correctly and securely. Where possible, old records should be shredded using an appropriate level of cross-shredding.

3.6 Data Protection Officer (DPO) / Compliance Officer

GDPR requires certain organisations appoint a dedicated, qualified and skilled Data Protection Officer (DPO).

A DPO is an independent officer of the organisation that reports to and advises senior management on all data protection matters that affect the organisation. A DPO has to have input on a wide range of activities and processes within the organisation: risk assessment, design (privacy by design & default), marketing, advertising, compliance, employment issues, etc. and acts as the single point of contract for a supervisory authority (Data Protection Commission). The organisation is required to publish and make public the identity and contact details of their DPO.

The following organisations are mandated to have a DPO under GDPR:

1. All public authorities and public bodies, including government departments, or,

2. Where the core activities of the organisation (data controller or data processor) consist of data processing operations, which require regular and systematic monitoring of individual on a large scale, or,

3. Where the core activities of the organisation consist of special categories of data (e.g. health data) or personal data relating to criminal convictions or offences.

We are not an organisation that engages in widescale systematic monitoring and processing of personal data, and special categories of personal data, and as such, we are not required to have a dedicated Data Protection Officer .

We are committed to data protection compliance and ensuring the privacy of all data subjects and have appointed the person named on the cover of this document as the organisation’s point of contact for all data protection matters.

3.7 Data Processing Agreements (DPA)

All organisations must have in place a data protection agreement with any other organisation that processes personal data on their behalf. Informal, ad-hoc or verbal arrangements are not acceptable; there must be a written agreement between a data controller and a data processor that address whether:

- the agreement is a ‘data processing agreement’ as per GDPR;
- the scope and categories of the personal data that will be processed by the processor;
- in the event of a data breach;
    - The data processor will notify the data controller without undue delay;
    - The data processor will cooperate with the data controller in investigating or rectifying any data breach;
    - The liability of the data processor;
- if appropriate, where data should be encrypted or subject to pseudonymisation;
- if applicable, whether the processor implements privacy by design or default;
- the data processer will deal with data access requests and how they will do it;
- both parties can show they are data protection compliant (by reviewing each other’s privacy policy, etc.);
- if applicable, make reference to any Privacy Impact Assessments carried out and any PIA solutions that need to be implemented before processing;
- a contact/DPO for the data processor; and,
- if applicable, the suitability of a Privacy Shield or onward transfer requirements.

As a data controller, we are required to have data processing agreements with any external third party that acts as a data processor. Each DPA would be unique and depends on the relationship and data processed by each separate data processor. A sample data processing agreement for use can be found at ***Schedule 1 - Annex 2: Data Processing Agreement (DPA) template*****.**

Our Privacy Policy, available on our website identifies our data protection and data processing practices to all data subjects and the public at large.

We may outsource some of our commercial activities to external third parties (e.g. accounting, debt collection, etc.) but as part of any terms of service with each third party there will be a contractual relationship regarding data processing (a data processing agreement).

We may on occasion act as a data processor in the provision of certain services to client. A sample data processing agreement for when acting as a data processor is contained in ***Schedule 1 - Annex 2: Data Processing Agreement (DPA) template.***

3.8 One Stop Shop (OSS) Agreements

The Data Protection Commission has issued guidelines as to a "One Stop Shop (OSS) Mechanism" for organisation that are established within the European Union and engaged in cross-border processing of personal data[5].

The main element required is the cross-border processing of personal data from an organisation in one EU country to at least one other EU country (or countries). If there is no international cross-border processing of personal data then the OSS mechanism does not apply but GDPR defines cross-border processing as:

- Processing of personal data which takes place in the context of the activities of an organisation in more than one Member State where that organisation is established in more than one Member State,

  Or

- Processing of personal data which takes place in the context of the activities of an organisation's single establishment but where that processing substantially affects or is likely to substantially affect data subjects in more than one Member State.

What is meant by 'substantially affects' is on a case-by-case basis and will depend on the nature of the processing activities the organisation is engaged in.

An organisation engaged in cross-border processing will have to establish its Lead Supervisory Authority (LSA) which is the data protection commission equivalent in that member state, e.g. the Irish Data Protection Commission equivalent in the UK is called the Information Commissioner. Any nominated Lead Supervisory Authority can deal with all data protection matters for the organisation.

The purpose of this is for an organisation to deal with only one supervisory authority for all data protection matters instead of having to deal with a supervisory authority in each EU country.

[5] https://www.dataprotection.ie/docs/OSS-Mechanism/k/1719.htm

We do not have offices or premises in another EU member state but we may use services providers located outside of Ireland, located in other EU member states, e.g. Microsoft Office, Zoom, etc. As such the One Stop Shop mechanism applies and the Lead Supervisory Authority is the Irish Data Protection Commission unless otherwise stated in any bespoke contract or data processing agreement for or with any applicable third party.

3.9 International Agreements / Privacy Shields

GDPR imposes restriction of the transfer of any personal data outside the European Economic Area (EEA) to other countries or to international organisations. These restrictions are in place to protect individuals' privacy by ensuring the same European standards (GDPR standards) are in place by requiring data sent to these countries or organisations to be subjected to the same restrictions, protections and security as if the data was processed within the EU.

In order to transfer any personal data outside of the EEA, the data subject must give explicit consent and there must be some form of detailed written agreement between the data controller within the EEA and the data processor located outside of the EEA that contains "adequate safeguards"

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the European Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority (Data Protection Commission) and approved by the European Commission;
- compliance with an approved code of conduct approved by a supervisory authority (Data Protection Commission);
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority (Data Protection Commission); or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority (Data Protection Commission).

We do not, in our own right, routinely transfer personal data outside of the EEA and, as such, there is no requirement to have in place any international agreements or privacy shield with any other agreement.

However, we may use third parties who help with operational/business functions of which some operate and store data outside of the EEA. Such third parties have in place as part of their respective terms of conditions and or data processing agreements binding corporate rules and or application of the EU-US Privacy Shield to ensure any data processed is processed in accordance with the EU General Data Protection Regulation and privacy rights are upheld through the entire process.

For example, we may use Mailchimp for processing marketing emails (but only if a data subject provides explicit consent to do so). Mailchimp has Standard Contractual Clauses (SCC) and an EU-US Privacy Shield Framework in place to ensure GDPR compliance. For Mailchimp's data protection practices please see their privacy policy available at www.mailchimp.com/legal/privacy.

For more information about the Privacy Shield Framework or Standard Contractual Clauses applicable to data being processed outside of Ireland and or the EU, please visit the Data Protection Commission website at www.dataprotection.ie.

Part 4: Rights of Data Subjects

4.1 Overview

Using general terms, data subjects have a number of rights under GDPR, the full detailed examination of which is beyond the scope of this policy. In short, the rights are, of which some have been previously addressed in this policy:

- Transparency and modalities.
- Information and access to personal data.
- Rectification and erasure.
- Right to object to automated individual decision-making.

We have identified our commitment to data protection transparency in ***Part 2*** of this policy.

4.2 Subject Access Request (AKA Data Access Request)

Article 15 of GDPR grants the right of data subjects to demand data controllers provide a wide range of information about the data subject's data (not just copies of the data itself) via a 'subject access request' or 'data access request'.

Any person has the right to make a request from a data controller as to whether or not personal data concerning that person is being processed, and, in such cases, **access to the personal data** and the following information:

a) The purposes of processing the personal data;
b) The categories of personal data held/processed;
c) The recipients or categories of receipt to whom the personal data have been or will be disclosed, in particular recipients in other countries or international organisations;
d) Where possible, the envisaged period for which the personal data stored will be stored, or, if not possible, the criteria use to determine that period;
e) The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) The right to lodge a complaint with a supervisory authority (which is the Data Protection Commission in Ireland);
g) Where the personal data was not collected from the data subject (originated from a third party) information as to the source of the personal data;

h) The existence of any automated decision-making, including profiling, and in such cases, meaningful information about the logic involved and the significance and the envisaged consequences of such processing for the data subject.

In cases where data is transferred to a third country or to an international organisation the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer (e.g. Privacy shield, Data Processing Agreements, etc.).

The data controller is entitled to ask the individual seeking the data request for identification so as to verify they are entitled to receive the data (e.g. copy of passport, etc.)

Our process

We are not entitled to impose a nominal charge on an individual making a subject access request and must provide the information within one month of receipt of the request.

In some cases, it may not be possible to complete the request within one month. In such cases, we must inform the data subject in writing, within one month of the initial request, that their request cannot be completed within a month, the reasons why and the expected time of completion. We then have two months from the date of the second letter to complete any access request.

In some cases, there may be an administrative burden or cost to us to complete the request. In such cases, we are entitled to notify the individual of the imposition of a ***reasonable*** charge if warranted, i.e. if the request is "manifestly unfounded or excessive", or if repetitive or additional copies of data are requested.

However, this is open to interpretation, has not been tested and is expected to be a very high threshold. In practice, we would have to justify the reasons for charging a fee to the Data Protection Commission but this invites additional scrutiny.

Any individual who wishes to make a subject access request / data access request they are to put their request in writing to:

Data Protection
Sustainability Matters CLG
The Black Church
St. Mary's Place
Dublin 7
D07 P4AX

Or by email, which is permitted under GDPR, to info@sustainablefinance.ie.

Any files sent to the person by email must be in a generally accepted accessible format (e.g. Word, pdf, jpeg, etc.).

A written data access request does not have to include the phrase 'data access request' or 'access request' nor does it have to state 'Article 15 of GDPR'; the data access request is valid so long as it is clear that the individual making the request is asking for their own personal data.

In response to the access request, we must provide the data subject with any exemptions listed in the next section and state that the individual has the right to refer the matter to the Data Protection Commission if they are unhappy with the outcome, however, we would ask the individual appeal the matter to us before contacting the Data Protection Commission as the matter may be easily resolved.

We must provide the contact details of the Data Protection Commission to the data subject, i.e. we must state in any response/letter to the individual:

> For more information please see the Data Protection Commission's website at www.dataprotection.ie or write to the Data Protection Commission at 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland.

Verbal data access requests or requests made over the phone will not be entertained as the requests must be in writing so we have a documented record of any access request.

There is no template provided for a data access request so each request will be dealt with and responded to on a case-by-case basis.

Important: Any response to an access request **must be reviewed** to ensure that no personal data relating to any other individual is included in the response as this would be a serious data breach. Any response must also be reviewed to ensure that none of the listed exemptions (detailed below) are included in the response.

4.3 Exemptions to a Data Access Request

GDPR states data controllers are entitled to reject (or charge for) a request that is "unfounded and or excessive" but this will be on a case-by-case basis and the threshold is expected to be very high. However, one example of excessive requests is repeated data access requests without a reasonable amount of time having passed.

If we feel a request is excessive, we are entitled to write to the individual and ask them to clarify what exactly they are looking for.

Under GDPR and Part 3, Chapter 3 of the Data Protection Act 2018, the following legitimate exemptions to a data access request apply:

- If the data is subject to legal professional privilege, meaning the data was created during a legal consultation with a lawyer or following legal advice from a lawyer, and/or the data was created specifically for an upcoming court case.

- Where the requester is involved in a claim against an organisation, seeking compensation and the information reveals details of the organisation's decision process in relation to their claim.

- If the information is held for statistical purposes, is not shared with any other person or organisation and cannot be identified as belonging to any particular individual (i.e. non-personal data).

- If releasing the data would mean that personal data about another individual would be unfairly disclosed. Personal data may be released in redacted form so as to protect the other individual's data.

- Where the data being sought involves personal opinions that have been expressed by another individual. Specifically, if the opinion was given in confidence, and it can be proven that the person providing the opinion at the time did so in the expectation of confidence, it does not have to be released. (If the opinion was given as part of regular business communications, does not involve personal opinions, and was given without the expectation of confidentiality, then it should be released).

- If the personal data has already been supplied in accordance with an access request, but identical requests continue to be made (unless new data has been created since the previous records were released, in which case the updated data must be provided).

- If the data that is requested is not the personal data of the requester, it cannot be released under an access request.

- If there is a legal confidentially imposed due to application of a specific statutory provision e.g. the personal data is considered part of a protected disclosure made in confidence under the Protected Disclosures Act 2014, a mandatory disclosure of a criminal offence under Section 9 of the Criminal Justice Act 2011, a disclosure under the Child First Act 2018, or any legitimate concerns or reporting relating to anti-money laundering regulations, etc.

If there is any doubt as to whether a disclosure relates to any legal proceedings, or potential threat of legal proceedings, or any mandated or protected disclosure refer the matter for expert or legal advice.

4.4 Rectification and Erasure

At any time, either on foot of a data access request or not, an individual may discover that the information held by the organisation is incorrect, inaccurate or out-of-date.

In such cases, the individual is entitled to have any incorrect personal data corrected, free of charge. They are also entitled to have any out-of-date information deleted or destroyed as soon as possible in accordance with the organisation's data retention policy.

For an individual to have their data corrected, deleted or destroyed they are to put their request in writing to:

Data Protection
Sustainability Matters CLG
The Black Church
St. Mary's Place
Dublin 7
D07 P4AX

Or by email to info@sustainablefinance.ie.

Verbal requests, or requests over the phone, to correct, delete or destroy any personal data will not be entertained. We require written confirmation from a data subject for any alteration or destruction of their personal data.

Requests to correct, delete or destroy data will be assessed by us on a case-by-case basis. In response, we will write to the individual, inform them of any decision made, any action taken and the reasons why.

We will also state to the data subject that they have the right to refer the matter to the Data Protection Commission if they are unhappy with the outcome, however, we ask the data subject to appeal the matter internally within our firm before contacting the Data Protection Commission.

Any request to correct, delete or destroy any personal data and any response, decision made, actions and correspondences will be retained by us in accordance with our Data Retention Policy.

4.5 Right to object to automated individual decision-making

A data subject has the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

We do not engage in any automated individual decision-making processes.

4.6 Data Portability

Article 20 of GDPR introduced the right of 'portability' in which data subjects have the right to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

This allows individuals to obtain and reuse their personal data for their own purposes across different services thereby taking advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.

The right to data portability only applies:

1. to personal data an individual has provided to a controller (no other data), and,

2. where the processing is based on the individual's consent or for the performance of a contract, and,

3. when processing is carried out by automated means.

We do not engage in automated processing and or automated decision-making processes therefore there is no requirement for us to provide data portability to an individual.

However, should a data subject want access to their personal data for the purposes of transferring it to another data controller, we will provide the data to the data subject in a commonly accessible format (e.g. doc file, pdf, jpeg, etc.) and the data subject can pass on their data to any third party they wish.

Part 5: Data Breach Management

5.1 Introduction

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted or unsecure environment. This includes instances in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so. Other names for a data breach include an 'unintentional information disclosure', a 'data leak' or a 'data spill'.

A data breach may occur for a number of reasons that include:

- Theft or loss of equipment on which data is stored (e.g. memory stick, laptop, etc.).
- Unprotected or easy access to organisational network or software (e.g. no password protection, etc.).
- Human error (e.g. sending an email to the wrong person, etc.).
- Access to information obtained via deception (e.g. 'social engineering' where someone pretends to be an authorised person to get information that allows them access secured data).

5.2 Management of a Data Breach (how to guide)

There are three main steps we use in dealing with a data breach.

1. Incident reporting,

2. Notification of data breach & risk assessment (including whether a breach must be notified to the Data Protection Commission),

3. Evaluation and Response.

5.2.1 Incident Reporting

Once an employee becomes aware of or suspects a data breach they are to report it to their line manager/supervisor and the designated person responsible for all data protection matters. This person is identified on the cover of this document.

In order to investigate properly, the following needs to be included, where possible, in any reporting of a data breach:

a) Date and time of the incident;
b) Date and time the breach was detected;
c) Description of the incident;
d) Who reported the incident and to whom;
e) The type and categories of data involved;
f) The number of individuals affected by the breach;
g) Whether the data was encrypted;
h) Details of any hardware or software involved (e.g. which computers, specific software involved, etc.); and,
i) Any corroborating or supporting materials.

5.2.2 Notification of Data Breach & Risk Assessment (Internal)

A data breach, or suspected data breach, must be reported to a line manager without delay who will in turn notify the organisation's nominated data protection person. The nominated data protection person will inform senior management and provide updates as appropriate.

A line manager or senior management in line with the organisation's nominated person, will assess the incident details and risks involved including:

a) What type and categories of data are involved?
b) How sensitive is the personal data involved, if any?
c) What protections were in place to reduce the risk of any breach?
d) How many data subjects have been affected by the breach?
e) What are the potential adverse effects for data subjects?
f) What is the likelihood of damage or loss to data subjects?
g) What is the potential damage to data subjects?

Details of the incident will be recorded in the organisation's Data Breach Register along with any supporting documentation (see ***Section 5.3: Data Breach Register***)

For every breach, we will decide as to whether the data breach is one that should be notified to the Data Protection Commission but we <u>still have to comply with the notification requirements in the next section even if there is no notification to the Data Protection Commission.</u>

In circumstances where there is no notification to the Data Protection Commission, we will keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. This record should include a brief description of the nature of the incident and an explanation of why the organisation did not consider it necessary to inform Data Protection Commission (see ***Section 5.3: Data Breach Register***).

These records should be kept for auditing, risk and compliance purposes (in order for the organisation to prove it did not breach GDPR or the Data Protection Act 2018).

5.2.3 'Notifiable Breach' & Data Protection Commission (External)

Under Article 33 of GDPR), a data controller "shall without undue delay and **within 72 hours**", notify a supervisory authority (the Irish Data Protection Commission) of any personal data breaches that are likely to result in a risk to the rights and freedoms of natural persons.

Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals **without undue delay**.

The GDPR term "data breaches that are likely to result in a high risk to the rights and freedoms of natural persons" is not defined but the Data Protection Commission has issued the following notification guidance[6] based on a 'Self-Declared Risk Rating' that mandates each organisation to self-declare the level of risk associated with any data breach. In practice, this requires each organisation to make a judgment call as to whether to report a breach to the Data Protection Commission and be able to prove the rationale for their decision.

In determining how serious we consider the data breach to be, and how it will affect data subjects involved, we have to consider the impact the breach could potentially have on individuals whose data has been exposed.

[6] https://www.dataprotection.ie/docs/GDPR-Overview/m/1718.htm GDPR May 2018 - Breach Notification

In assessing this potential impact, we should consider the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place and whether the personal data of vulnerable individuals has been exposed.

We then establish the level of risk involved using the four categories identified by the Data Protection Commission[7]:

- ***Low Risk:*** The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal

- ***Medium Risk:*** The breach may have an impact on individuals, but the impact is unlikely to be substantial

- ***High Risk:*** The breach may have a considerable impact on affected individuals

- ***Severe Risk:*** The breach may have a critical, extensive or dangerous impact on affected individuals.

Note: If we establish there is no risk then there is no requirement to notify the Data Protection Commission but there is a requirement to keep records of the details, the means for deciding there was no risk and who decided there was no risk.

Initial notification of breach

There are two different ways to notify a breach to the Data Protection Commission.

The first is using their online reporting form available at www.dataprotection.ie which requires all relevant data processing information at the time of reporting. The difficulty with the online reporting is that you need all the required information upfront but you are not informed what you need until you progress through the reporting form.

The second is via a special reporting form that you can emailed to the Data Protection Commission. The forms were formerly available on the Data Protection Commission's website www.dataprotection.ie but now must be requested from the Data Protection Commission.

Regardless of which method you use, the information required is the same and it is up to the data controller/processor to prove compliance throughout each step of the reporting procedure and justify why you reported it to data subjects or not.

[7] https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification

Online notification of a data breach to the Data Protection Commission

The simplest method of reporting a data breach to the Data Protection Commission is via their online reporting form at https://forms.dataprotection.ie/breach-notification. You will need to have information about the breach, who was affected, what happened, the number of data subjects involved and the categories of personal data, the risk you attributed to the breach along with what you did to minimise any damage to data subjects.

Email method of notification

Breach notification forms can be emailed to the Data Protection at this email address breaches@dataprotection.ie

All national breach notifications must be notified using the 'National Breach Notification Form' (see ***Schedule 1 – Annex 4***).

All cross-border personal data breaches must be notified using the 'Cross-Border Breach Notification Form' (see ***Schedule 1 – Annex 4***).

Cross-border processing means either:

- Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of an organisation (i.e. if the organisation has branches/subsidiaries in Ireland and another EU or EEA country); or

- Processing of personal data which takes place in the context of the activities of a single establishment of an organisation that substantially affects or is likely to substantially affect data subjects in more than one Member State (i.e. if the organisation is only based in Ireland but processes personal data from people in at least one other EU or EEA country).

The Data Protection Commission uses the subject line of emails to assign priority in response times and have issued guidance on what to put in the subject line of emails to breaches@dataprotection.ie.

In the subject line of the email please include the following information:

- Whether the breach you wish to notify DPC of is 'new' or an 'update' to a previous breach notification.

- Your firm's name

- The organisation's self-declared risk rating for the breach.

In practice, the subject line of the email should read as:

Subject: New Breach Report, NAME, Low Risk
[or insert appropriate level of risk]

The Data Protection Commission will respond in due course with a reference number.

Do not include or attach any personal data or information about any data subject or affected individual in a breach notification to the Data Protection Commission.

Updating a notification of breach

If the notification was incomplete for any reason, the organisation should submit further information when it becomes available.

For updated notifications include the following information in the subject line of the email:

- Updated Breach Notification
- Organisation Name
- DPC reference number (if one has been provided)
- The self-declared risk rating for the breach

In practice, the subject line of the email should read as:

Subject: Updated Breach Report, NAME, [Ref. Number], Low Risk
[or insert appropriate level of risk]

The Data Protection Commission will respond in due course.

In practice, it is simpler for data controllers to use the online reporting form on www.dataprotection.ie then using the email method of report.

5.2.4 Notifying Data Subjects

Under Article 34 of GDPR, all organisations must notify data subjects "**without undue delay"** of any breach that has affected their data where the breach "**is likely to result in a high risk to the rights and freedoms of a data subject**"

If we are considering notifying data subject of a breach then we should have already established the level of risk to data subjects and can justify our rationale for arriving at that level of risk (that is also notifiable to the Data Protection Commission as per the previous section).

All affected data subjects are to be contacted by us and informed of,

a) a brief outline of the data breach using clear and plain language;
b) the personal data, types and categories of data concerning the data subject that was subject to the breach;
c) suggested steps that the data subject might take to ensure the safety of the data subject (e.g. change passwords, etc.);
d) the fact the organisation has notified the Data Protection Commission of the breach; and,
e) any steps taken by us to rectify the situation.

If the data is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it (e.g. encrypted) then there may be no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures were of a high standard, e.g. whole-disk encryption of 256-bit strength, etc.

However, in cases where we are acting as a data processor, the data controller must be made aware of any data breach and the outcome of any internal investigation by us. The data controller will then respond accordingly on a case-by-case basis.

5.2.5 Data Protection Commission's role following a Notifiable Breach

Following a notifiable breach, should the Data Protection Commission request us to provide a detailed written report of the incident, they will specify a timeframe for the delivery of the report based on the nature of the incident and the information required.

Such a report should be similar to our own breach register of the breach and should reflect careful consideration of the following elements:

a) a chronology of the events leading up to the loss of control of the personal data;
b) the amount and nature of the personal data that has been compromised;
c) the action being taken to secure and / or recover the personal data that has been compromised;
d) the action being taken to inform those affected by the incident or reasons for the decision not to do so;
e) the action being taken to limit damage or distress to those affected by the incident; and,
f) the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the Data Protection Commission may investigate the circumstances surrounding the breach.

Investigations may include on-site examination of systems and procedures and could lead to a recommendation to provide data subjects with information about the Commission's findings.

All management, employees, sub-contractors and data processors are required to fully cooperate in any investigation by the Data Protection Commission.

5.2.6 Evaluation Response

Following any data breach, notification, enquiry or investigation from the Data Protection Commission a review of the incident will be made by the organisation with oversight from senior management.

The purpose of this review is to:

a) ensure that any or all steps taken during the incident were appropriate under the circumstances;
b) ensure a record of any and all measures being taken to prevent repetition of the incident is kept;
c) identify any areas that can be improved and make recommendations of same;
d) document any recommended changes to policy and or procedures; and,
e) implement any recommended changes to policy and or procedures as soon as possible.

5.3 Data Breach Register

All organisations are required to have a data breach register which registers the particulars of any data breach. This register is not available to the public and may contain commercially sensitive information about our internal processes, procedures or services.

This register is also used to review our risk assessment policy (for any risks that may have materialised) and or any corporate risk assessment strategies and is confidential.

The register is kept secure and confidential as details of a breach will, by necessary, contain particulars of personal data that was affected.

The register will be made available to our point of contact for all data protection matters and senior management as part of any risk assessment, auditing or governance reviews. It will also be made available to the Data Protection Commission upon request.

In the event we act as a data processor, then the data controller may be entitled to have access to any breach register and associated documents for compliance/auditing purposes.

Part 6: Awareness Training & Support for Staff

6.1 Introduction

We endeavour to support all employees who process personal data through Data Protection Awareness Training and Data Protection Support.

6.2 Data Protection Awareness Training

Data Protection Awareness Training will take place during induction of new employees and at various periodic intervals through their time with us. Training will also be provided at any important change or development in data protection legislation or best practices as the case may be.

As part of any Data Protection Awareness Training, a familiarity and understanding of this Data Protection Policy is required.

Any updates in legislation and best practices will be incorporated into the next review of this Data Protection Policy.

Any relevant guidance notes or press releases from the Data Protection Commission are to be inserted into ***Schedule 1 – Annex 5*** and to be incorporated into the next policy review.

All employees are required to regularly review ***Schedule 1 – Annex 5*** which is incorporated into this policy.

6.3 Data Protection Support

Data protection support is provided by the person identified on the cover of this document who will be able to assist any employee with any question or query they may have in relation to any data protection mater.

Conclusion

This Data Protection Policy shall be reviewed at regular periodic intervals to ensure that it complies with current data protection legislation and best practice. It shall also be reviewed to ensure it remains comprehensive and easy to understand.

Date of review

The next date of review for this document is March 2024 or upon the introduction of the final text of the ePrivacy Regulations or upon the Privacy Shield replacement being implemented, whichever is sooner.

Schedule 1 - Annex 1: CCTV, Webcams & Dashcams

Introduction

At time of drafting, we do not use CCTV cameras in our premises but reserve the right to do so for a number of legitimate purposes including;

> As a preventative measure and deterrent against, and or the investigation of, any act or omission that may affect the health, safety and wellbeing of any individual on the organisation's premises.
>
> As a preventative measure and deterrent against, and or the reporting and or investigation of, any criminal act or omission that will be reporting to the relevant authorities.

CCTV footage may be used in the investigation of any matter relating to the any grievance procedure, and, in such cases where an investigation concludes that an employee acted inappropriately under the circumstances and or was in breach of any policy, then CCTV footage may be used as basis for, and or a consideration that may be taken into account for, any disciplinary action taken by the organisation against that employee.

CCTV footage may also be used for the reporting of any offence, crime, health and safety violation and or for the purpose of obtaining legal advice and or engaged in legal proceedings relating to any person on our premises; Such persons may include employees, contractors, visitors and trespassers on our premises.

Consent for CCTV

1. Members of the public (including visitors to our premises)

All CCTV cameras must be visible; they cannot be hidden. At <u>every</u> entrance onto the premises to which CCTV is monitored and recorded by or on behalf of the organisation, there needs to be visible signs that state:

> 1. CCTV is monitored and recorded for the health, safety and wellbeing of employees and visitors to the premises (or words to that effect).
>
> 2. The identity of the Data Controller.

3. The Data Controller’s contact details (phone number and website address).

4. The Data Controller’s Privacy Policy (or Data Protection Statement) is available online and provide the website address.

2. Our employees

The same conditions above apply to all employees but the following additional factors apply.

Contracts of employment includes compliance with a data protection policy and use of CCTV in accordance with those policies. The use of CCTV footage may be used in any grievance and disciplinary procedure for or against any employee.

For the avoidance of any doubt, CCTV footage can be used at the basis for initiating a complaint, grievance or disciplinary procedure against any employee.

For avoidance of any doubt, our premises are considered ‘working environments’ and the monitoring and recording of images is lawful to comply with the provisions of the Health, Safety and Welfare at Work Acts.

Retention of CCTV footage

CCTV footage is automatically deleted by being recorded over after a period of time. The specific period of time is commercially sensitive information but is considerably less than the general seven year data retention policy referred to the main body of Data Protection Policy and is typically 4-6 weeks.

CCTV may be identified and retained, i.e. not subjected to automatic deletion, for any matter permissible under this Data Protection Policy. In such cases, CCTV footage will be kept in accordance with our data retention policy (i.e. held in secure environment, not kept for any longer than necessary, regularly reviewed, etc.).

CCTV footage will not be shared with any third party without authorisation by senior management (or data protection officer/compliance officer authorised to make data protection decisions) and is only to be shared for a specific purpose (e.g. to obtain legal advice, in order to report a crime, etc.). In such cases, a record of what data was shared, to whom and the reasons why are to be recorded on file.

Any breach of the Data Protection Policy relating to CCTV footage may be the basis for a grievance procedure and or disciplinary procedure against an employee and may also be considered “gross misconduct” and may lead to dismissal.

CCTV of Accidents

The Safety, Health and Welfare at Work (General Application) Regulations 2007 (S.I. No. 299 of 2007) mandates an employer must report and investigate certain accidents in the workplace.

As part of this investigation process, we must retain certain information relating to an accident, e.g. parties involved, causes, investigation, outcome, CCTV footage (if available) for a period of **ten years**.

Section 226 of The Safety, Health and Welfare at Work (General Application) Regulations 2007 (S.I. No. 299 of 2007) as, inserted by Section 6 of Safety, Health and Welfare at Work (General Application) (Amendment) (No. 3) Regulations 2016 (S.I. No. 370 of 2016), specifically states a mandatory ten-year period to retain records relating to a relevant accident.

Relevant CCTV footage of a relevant accident may be subject to a ten-year retention period.

Webcams & Voice over Internet (VoIP)

We use webcams and voice over internet (VoIP) for communicating with clients, employees and various third parties.

Communications online are **not to be recorded without the knowledge and explicit consent of all parties** to the communication (*i.e.* both sides of a conference call). Any recordings, screenshots, files received or shared, or associated personal data, can retained in accordance with the organisation’s data retention policy.

We may use collaborative communications tools including but not limited to Skype, Zoom, WebEx or Facebook Face Time for webcam communications, of which all organisations are located outside of the EU but purport to have an EU-US Privacy Shield in place to ensure GDPR compliance and protect the rights of all data subjects.

Dash cams

We do not own or operate any vehicles with dash cams.

Requests from An Garda Síochána for footage

The Data Protection Commission have drawn a distinction between An Garda Síochána making a request to view CCTV footage (or any footage) at an organisation's premises and An Garda Síochána requesting a copy of CCTV footage to take away[8].

In essence, the Data Protection Commission has indicated that a request by a member of An Garda Síochána to view footage at the organisation's premises is unlikely to raise any data protection concerns.

However, a request by a member of An Garda Síochána to copy footage which will be then taken off the premises may cause data protection concerns. In such cases, the Data Protection Commission advises to get a written request from a member of An Garda Síochána before allowing them to copy the footage. The reason for this is to ensure that data controller has a written record of why they shared data (footage) with a third party (An Garda Síochána) and this should be kept on file to show compliance with the Data Protection Act 2018 in the event of it becoming an issue.

If a member of An Garda Síochána has a warrant or a court order for any footage then it must be given without delay (as the lawful basis for sharing the data is on foot of a warrant or court order).

In summary, if a member of An Garda Síochána wants to copy footage, please ask them to submit their request in writing so it can be kept on file. If they have a warrant or court order, then they are entitled to take the footage.

[8] https://www.dataprotection.ie/docs/Data-Protection-CCTV/m/242.htm

Schedule 1 - Annex 2: Data Processing Agreement (DPA) Template

Please note there are two data processing agreements on file.

The first is where we are acting as a data controller (where we are ultimately in control of the data and or the data originated from us) whereas the second is where we act as a data processor (acting on behalf of some a third party and using the data for their purposes).

Each Data Processing Agreement must be amended to include the categories of personal data being processed.

1. Where we are the data controller

DATA PROCESSING AGREEMENT

This agreement is between:

On the first part, for Sustainability Matters CLG t/a International Sustainable Finance Centre of Excellence of The Black Church, St. Mary's Place, Dublin 7, D07 P4AX (hereby referred to as 'data controller'), and,

On the second part **[INSERT NAME AND ADDRESS OF THIRD PARTY]** (hereby referred to as the 'data processor').

IT IS HEREBY AGREED BETWEEN THE PARTIES THAT:

1. The purpose of this agreement is to ensure compliance with the General Data Protection Regulation (GDPR) and any associated data protection legislation.

2. This Agreement shall in all respects be governed by and interpreted in accordance with the laws of the Republic of Ireland.

3. The parties submit to the exclusive jurisdiction of the Irish Courts and the Irish Data Protection Commission for the purposes of this Agreement and associated data protection related matters.

4. Interpretation of any word or phrase in this agreement is to be interpreted based on the wording used in the Data Protection Act 2018 unless otherwise stated to the contrary.

5. The data processor is only authorised to process personal data only on the basis of the authorisation and instruction received from the data controller.

6. The data processer cannot use any personal data that originated from the data controller for their own use. The only exception to this may be exemptions being permitted under law (e.g. mandatory reporting of certain criminal offences, etc.).

7. The data controller will ensure that data is transferred or given to the data processer with reasonable security measures are in place to secure the data from any unauthorised access or disclosure.

8. The data processer will ensure reasonable security measures are in place to protect personal data from any unauthorised access or disclosure as it is being processed.

9. The data processor indemnifies the data controller for any loss or liability, and nor any claim of such by a data subject, as a result of the data processor breaching GDPR and or the Data Protection Act 2018.

10. The data processor will provide the data controller access to their data protection policies, practices and or procedures for the purposes of complying with any data protection audit as requested or initiated by the data controller.

11. At the time of entering this agreement, the categories of data the data processer may process on behalf of the data controller are, but may be changed by mutual agreement:

    - **[INSERT CATEGORIES OF DATA YOU ARE SHARING AND WHY IT IS BEING SHARED]**
    - *E.g. Names, addresses, phone numbers and email addresses of your clients in order for the sub-contractor/data processer to send them marketing information.*
    - *E.g. names, addresses, phone numbers, email addresses and accounts of your clients who have not paid invoices in order for the sub-contractor/data processor to act as debt collector and collect money from outstanding accounts.*
    - *E.g. names and email addresses of your sales leads so the sub-contractor/data processer can invite them to a sales event, etc.*

12. The data shall be retained by the data processor in accordance with the data controller's data retention policy that is part of the data controller's data protection policy except upon termination of this agreement.

13. Upon the termination or ending of this agreement all personal data will be returned to the data controller or deleted or destroyed, including any data held in 'back up' or storage facilities, with the exception of any data held in according with statutory or legal requirement.

14. The data processer shall notify the data controller without undue delay in the event of any data breach, including details of any unauthorised access or disclosure.

15. The data processer shall notify the data controller, without undue delay, in the event of any person making a data access request and the information sought.

16. The data processor shall ensure that it has appropriate employee procedures in place to ensure compliance with GDPR and any breach of data protection legislation by an employee, is a basis for a grievance and disciplinary procedure to be initiated against the employee.

17. The data processer shall familiarise themselves with the data controller's privacy policy.

Signature ____

Signed on behalf of the data controller: Sustainability Matters CLG

Printed name and position:

____

Date:

____

Signed on behalf of the data processor:

____

Printed name and position:

____

Date:

____

2. Where we are the data processor

DATA PROCESSING AGREEMENT

This agreement is between:

A. On the first part **[INSERT NAME AND ADDRESS OF THIRD PARTY]** (hereby referred to as the 'data controller').

   and

B. On the second part, Sustainability Matters CLG t/a International Sustainable Finance Centre of Excellence of The Black Church, St. Mary's Place, Dublin 7, D07 P4AX (hereby referred to as the 'data processor').

IT IS HEREBY AGREED BETWEEN THE PARTIES THAT:

1. The purpose of this agreement is to ensure compliance with the General Data Protection Regulation (GDPR) and any associated data protection legislation.

2. This Agreement shall in all respects be governed by and interpreted in accordance with the laws of the Republic of Ireland.

3. The parties submit to the exclusive jurisdiction of the Irish Courts and the Irish Data Protection Commission for the purposes of this Agreement and associated data protection related matters.

4. Interpretation of any word or phrase in this agreement is to be interpreted based on the wording used in the Data Protection Act 2018 unless otherwise stated to the contrary.

5. The data processor is authorised to process personal data originating from the data controller on the basis of consent and instruction received from the data controller for the fulfilment of a contractual obligations between the parties.

6. The data processer cannot use any personal data that originated from the data controller for their own use. The only exception to this may be exemptions being permitted under law (e.g. mandatory reporting of certain criminal offences, etc.).

7. The data controller will ensure that data is transferred or given to the data processer with reasonable security measures are in place in secure the data from any unauthorised access or disclosure.

8. The data processer will ensure reasonable security measures are in place to protect personal data from any unauthorised access or disclosure as it is being processed.

9. At the time of entering this agreement, the categories of data the data processer may process on behalf of the data controller, that originated form the data controller are, but may be changed by mutual agreement:

   - **[INSERT CATEGORIES OF DATA BEING SHARED WITH YOUR COMPANY AND WHY IT IS BEING SHARED]**
   - *E.g. Names, addresses, phone numbers and email addresses of clients in order for us (as data processer) to send them marketing information.*
   - *E.g. names, addresses, phone numbers, email addresses and accounts of clients who have not paid invoices in order for the us (as data processor) to act as debt collector and collect money from outstanding accounts.*
   - *E.g. names and email addresses of sales leads so we (as data processor) can invite them to a sales event, etc.*

10. The data shall be retained by the data processor in accordance with the data controller's data retention policy that is part of the data controller's data protection policy except upon termination of this agreement.

11. Upon the termination or ending of this agreement all personal data will be returned to the data controller or deleted or destroyed, including any data held in 'back up' or storage facilities, with the exception of any data held in according with statutory or legal requirement.

12. The data processer shall notify the data controller without undue delay in the event of any data breach, including details of any unauthorised access or disclosure.

13. The data processer shall notify the data controller, without undue delay, in the event of any person making a data access request and the information sought.

14. The data processor shall ensure that it has appropriate employee procedures in place to ensure compliance with GDPR and any breach of data protection legislation by an employee, is a basis for a grievance and disciplinary procedure to be initiated against the employee.

15. The data controller shall familiarise themselves with the data processor's privacy policy available.

Signature: ______________________________

Signed on behalf of the data controller: ______________________________

Printed name and position: **[INSERT THIRD PARTY NAME HERE]**

Date: ____________________

Signature: ____

Signed on behalf of the data processor: Sustainability Matters CLG

Printed name and position: ____

Date: _________________

Schedule 1 - Annex 3: Health & Safety matters

Health and safety of employee's straddle employment legislation, health and safety legislation and data protection legislation.

Accidents/Injuries

The Safety, Health and Welfare at Work (Reporting of Accidents and Dangerous Occurrences) Regulations 2016 mandate employers to report certain accidents and dangerous occurrences to the Health and Safety Authority. The full reporting conditions are beyond the remit of this Data Protection Policy.

In order to report, an employer may be required to share some personal data of those involved and/or high-level medical data in order to report the severity of any accident or injury, usually after some form of investigation. In such cases, this Data Protection Policy applies to all steps involved in complying with all Health & Safety requirements, e.g. from the initial investigation and reporting stage right through to the final outcome and storage/filing of the report.

Data retention relating to certain accidents

The organisation identifies that data relating to certain accidents is excluded from the organisation's general data retention policy of eight years.

Section 226 of The Safety, Health and Welfare at Work (General Application) Regulations 2007 (S.I. No. 299 of 2007) as, inserted by Section 6 of Safety, Health and Welfare at Work (General Application) (Amendment)(No. 3) Regulations 2016 (S.I. No. 370 of 2016), specifically states a mandatory ten year period to retain records relating to a relevant accident.

All records, including personal data, relating to a relevant accident is subject to a mandatory ten-year retention period under the above regulations. At the end of the mandatory retention period all records will be destroyed except in the event on any ongoing legal action that necessitates their retention.

Sick Leave/Medical Certificates

Subject to an employee's contract of employment and employee handbook, employees are required to certify short-term medical absences from work or short-term sick leave' via a 'high level' report or note from a qualified doctor. The purpose of such a 'high level' report or note is to identify whether in the opinion of a medical expert that an employee was unfit for work for specific dates and also identifies when, in that expert's opinion, an employee is fit for work (at the expiration of the 'sick leave'). Medical certificates should not go into any further details.

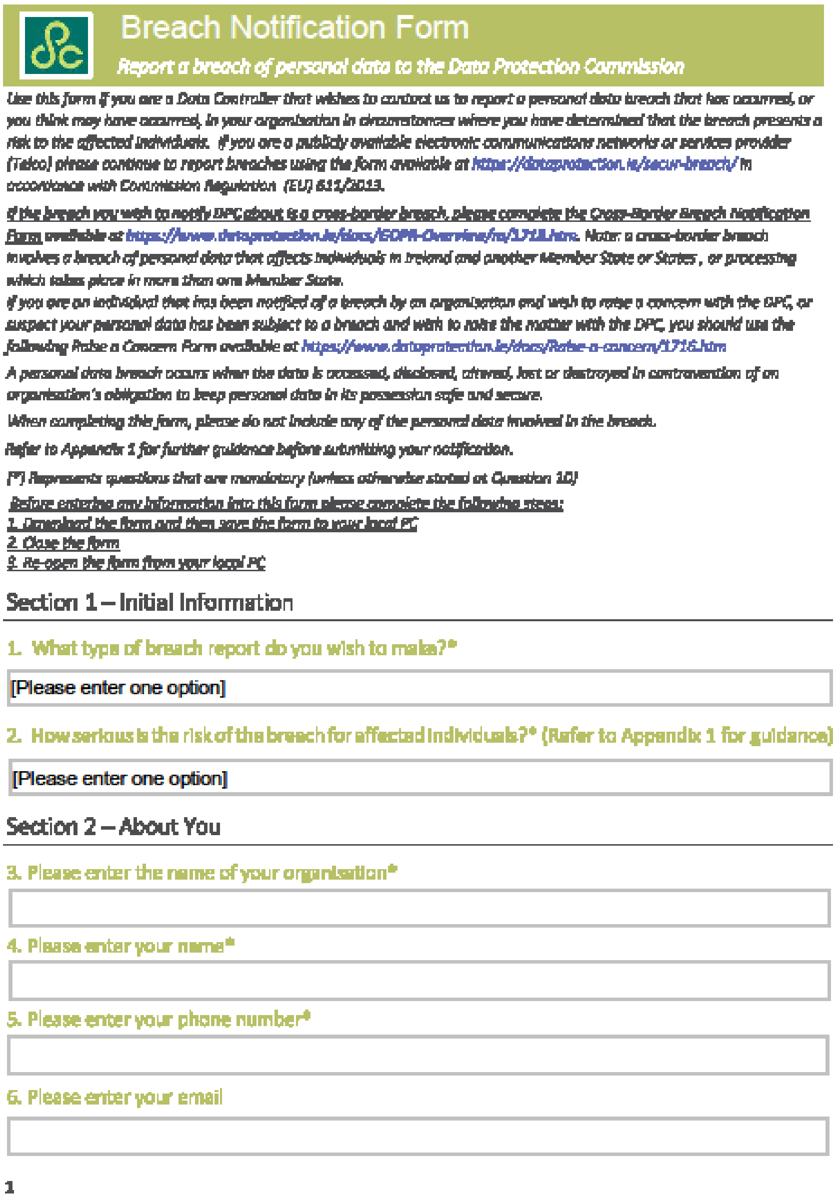
The processing of any medical reports or sick leave reports will be conducted in accordance with the Data Protection Policy. As such, any relevant medical notes or reports are stored in a secured physical location with limited access and are destroyed once no longer necessary.

Schedule 1 – Annex 4: Data Protection Commission Forms

The Data Protection Commission has issued the following forms to be used as appropriate.

1.4.1: Data Breach Notification (within Ireland)

The Data Protection Commission has an online form for reporting any data beach. In the event the DPC website is not working, email info@dataprotection.ie and request a form.



Breach Notification Form

Report a breach of personal data to the Data Protection Commission

Use this form if you are a Data Controller that wishes to contact us to report a personal data breach that has occurred, or you think may have occurred, in your organisation in circumstances where you have determined that the breach presents a risk to the affected individuals. If you are a publicly available electronic communications networks or services provider (Telco) please continue to report breaches using the form available at https://dataprotection.ie/secur-breach/ in accordance with Commission Regulation (EU) 611/2013.

If the breach you wish to notify DPC about is a cross-border breach, please complete the Cross-Border Breach Notification Form available at https://www.dataprotection.ie/docs/GDPR-Overview/ro/1718.htm. Note: a cross-border breach involves a breach of personal data that affects individuals in Ireland and another Member State or States , or processing which takes place in more than one Member State.
If you are an individual that has been notified of a breach by an organisation and wish to raise a concern with the DPC, or suspect your personal data has been subject to a breach and wish to raise the matter with the DPC, you should use the following Raise a Concern Form available at https://www.dataprotection.ie/docs/Raise-a-concern/1716.htm

A personal data breach occurs when the data is accessed, disclosed, altered, lost or destroyed in contravention of an organisation's obligation to keep personal data in its possession safe and secure.

When completing this form, please do not include any of the personal data involved in the breach.

Refer to Appendix 1 for further guidance before submitting your notification.

(*) Represents questions that are mandatory (unless otherwise stated at Question 10)

Before entering any information into this form please complete the following steps:
1. Download the form and then save the form to your local PC
2. Close the form
3. Re-open the form from your local PC

Section 1 – Initial Information

1. What type of breach report do you wish to make?*

[Please enter one option]

2. How serious is the risk of the breach for affected individuals?* (Refer to Appendix 1 for guidance)

[Please enter one option]

Section 2 – About You

3. Please enter the name of your organisation*

4. Please enter your name*

5. Please enter your phone number*

6. Please enter your email

1

1.4.2: Cross-border Breach Notification

The Data Protection Commission has an online form for reporting any data beach. In the event the DPC website is not working, email info@dataprotection.ie and request a form.

Cross-Border Breach Notification Form

Contact the DPC in relation to a breach that involved cross-border processing

Use this form if you are a Data Controller that wishes to contact us to report a cross-border personal data breach that has occurred, or you think may have occurred, in your organisation in circumstances where you have determined that the breach presents a risk to the affected individuals. If you are a publicly available electronic communications networks or services provider (Telco) please continue to report breaches using the form available at https://dataprotection.ie/secur-breach/ in accordance with Commission Regulation (EU) 611/2013.
A cross-border breach involves a breach of personal data that affects individuals in Ireland and another Member State or States, or processing which takes place in more than one Member State.
If you are an individual that has been notified of a breach by an organisation and wish to raise a concern with the DPC, or suspect your personal data has been breached and wish to raise the matter with DPC, you should use the Raise a Concern Form available at https://www.dataprotection.ie/docs/GDPR-Overview/m/1718.htm.
A personal data breach occurs when the data is accessed, disclosed, altered, lost or destroyed in contravention of an organisation's obligation to keep personal data in its possession safe and secure. When completing this form, please do not include any of the personal data involved in the breach. For example, do not include names of individuals impacted by the breach. Should we require this information, we will request it at a later date.
Note: Where you determine there is no risk, keep a record internally of the details, the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded.

If you want to update a breach notification report you previously sent to DPC, please complete Section 0, Section 1 and Section 9. If changes are required to other sections, please also complete these sections.

Please send this form to: breaches@dataprotection.ie. [*] Represents questions that are mandatory

Refer to the Article 29 Breach Guidelines for further information - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Before entering any information into this form, please complete the following steps:
1. Download the form and then save the form to your local PC
2. Close the form
3. Re-open the form from your local PC

Section 0 – Data Breach Notification:

0. Please enter the ID of the breach

1. About you:

1.1 Contact Details

1.1A Name and function of the person who can be contacted for more information about the breach:

1.1B Contact details (including your phone number and email address):

1

Schedule 1 - Annex 5: Updates

This annex is reserved for guidance notes and press releases from the Data Protection Commission.

Any guidance notes and or press releases are to be inserted into this annex so as to enable your organisation to keep up to date of current data protection matters.

Any materials inserted into this annex will be reviewed at the next review date of the data protection policy to in order to incorporate them into the next version of the data protection policy.

Schedule 2 - Annex 1: Privacy Impact Assessments

People have expectations of privacy. If you provide your personal data for someone to use, you expect them to keep it safe, secure and confidential, especially if the information was personal. Similarly, GDPR requires organisations to consider how a person's data will be processed and to, effectively, consider how people would feel about their data being processed in a particular manner.

If an organisation is considering a new project (or changing/expanding a current project) it has to consider whether it will impact upon individuals' privacy and, if so, the effect it could have. In order to do this, organisations are required to consider, and if appropriate, create a Privacy Impact Assessment (PIA).

Whether a PIA is required for a particular project must be considered on a case-by-case basis. Using general terms, a screening process can be a good indicator as to whether a full PIA is required.

The screening process should be conducted by the organisation's data protection officer(s) or compliance officer(s) in conjunction with any project lead and any people who can advise on the technical or practical processes in which this project will use personal data.

IMPORTANT:

1. Please refer to your organisation's Data Protection Policy and your internal point of contact for all data protection matters for terms used or if you are unsure of what something means.

2. The Data Protection Commission have issued guidelines as to when a PIA is required. Please review ***Section 3.3 – Privacy Impact Assessments (PIA)*** of this policy and the Data Protection Commission's website www.dataprotection.ie for any updates to PIA requirements.

PIA Screening

The term ‘project’ means any project, initiative, services or product the organisation is considering creating, launching, expanding upon or altering an existing one.

1. Does this project fall within the categories of processing that mandate a PIA as per ***Section 3.3 – Privacy Impact Assessments (PIA)***?

2. Would the project raise privacy concerns or expectations about data people would generally consider private (e.g. medical records, political views, location, etc.)?

3. Are you using or going to use personal data for the purpose it was collected or in a way that it is currently not being used?

4. Will this project require you to contact individuals (e.g. marketing, targeted adverts, etc.)?

5. Will data about individuals be disclosed to any third parties that previously not had access to that data?

6. Does the project involve the use of new technology that could be considered as being intrusive to a person’s privacy (e.g. facial recognition, tracking software, etc.)?

7. Will this project cause you to make any decisions to take any action against any individuals that could significantly impact upon them?

8. Does this project rely on any fully automatic processing of data or any automated decision-making processes?

9. Does this project require any third party to act as a data processor for you (as a data controller)?

If you answered no to all of the above and you can provide evidence to support your answers then it would be a good indicator that a PIA is not required.

If you are not sure about an answer, then you must conduct a PIA to ensure your organisation is data protection compliant.

This screening document, with any attached evidence, should be kept on file for auditing and compliance purposes in accordance with the organisation’s data retention policy.

If the initiate changes at any stage, you must complete the screening process again to ensure data protection compliance.

What should be in a Privacy Impact Assessment (PIA)?

In general terms, the PIA should:-

- set out the objectives of the new process or product;
- explain why you feel a PIA is necessary;
- map data flows (i.e. what data is being processed, where does it originate and where does it go, etc.);
- identify the risks to individual's privacy in terms of security, and as potential threats to confidentiality, integrity or availability;
- clarify the legal basis for processing data;
- identify and evaluate the privacy solutions (how can you reduce or remove the risk?);
- sign off and record the PIA outcomes;
- integrate the outcomes into the project plan; and,
- consult with internal and external stakeholders, as needed, throughout the process.

Who should conduct the PIA?

A PIA needs input from people with wide ranges of skills who know and understand the new initiative or project, how it can affect people's data, how it fits into the organisation's culture and how it fits into the existing governance and risk assessment framework of the organisation. In short, a diverse team is required with at least one qualified data protection officer or compliance officer who, as part of a team, map out the data processes and establish that each step along the process complies with data protection legislation.

Do I need a PIA?

As stated, the Data Protection Commission have mandated a PIA for certain processing activities as outlined in ***Section 3.3 – Privacy Impact Assessments (PIA*****).** Regardless, if this screening process indicates that you need a PIA then you probably need one.

A failure to provide a PIA when required, or when audited by the Data Protection Commission, may be a serious breach of the data protection legislation.

Schedule 2 - Annex 2: PIA Template

1. Background Information

Project name:
PIA compiled by (name and title):
Contact details of compiler:
Names of contributors to PIA:
Date PIA was completed:

Note: The examples used are based on outsourcing your debt collection to a subsidiary (third party).

2. Outline the project and why the need for a PIA was identified

For example: concerns over a specific breach, unsure as to the relevance of data, etc.

Please attach any relevant supporting documents.

E.g. This project involves our company sharing personal data with our subsidiaries, who are separate legal entities but trade under our umbrella brand / trading name. One subsidiary is responsible for debt collection and we share data with this subsidiary in order to collect outstanding monies, etc.

3. Please identify the categories of personal data, including any special categories of personal data, that will be processed and why they will be processed.

List any individuals or groups of individuals to whom the data relates, what the data is (names, addresses, etc.) and why the data must be processed.

E.g. We identify individuals who are more than 90 days outstanding on payment, we identify their names, addresses, email addresses and phone numbers (in order to contact them over payment), account details (to prove the debt), payment details (to prove the debt remains outstanding), date of birth (for verification purposes).

The special categories of personal data that will be processed are: financial data and personalised email addresses (e.g. name.surname@example.com), etc.

This data will be sent to the subsidiary, in accordance with the company privacy policy, for the subsidy to act as debt collector so the company can get paid.

4. Please identify the legal basis relied upon to process personal data.

Identify in detail each ground you're relying upon to process personal data (there may be multiple grounds). If relying on consent, please identify how consent was obtained.

E.g. Grounds relied upon are consent and processing in order to fulfil contractual obligations.

Clients apply for credit facilities via an application form that was subject to the company's privacy policy. A copy of the standard application form is attached and shows that a client consents to data processing, by actively ticking a box stating that they agree to the company's privacy policy, by signing the application form...

5. Please outline how the data will flow within the organisation and/or with any third parties.

Detail the collection, use, storage and deletion of personal data. Drawing a diagram may help identify data flows. Please include how many individuals are likely to be affected by any data flow.

E.g. The company will pass the aforementioned data to the subsidiary who in turn will process the data to contact each customer...

6. How you will identify privacy risks.

Details the steps you will take to identify and address any risk to privacy. This includes who you consult within your organisation, any consultations with external third parties, and how you carried out or will carry out any consultation.

E.g. We consulted with the customer care team to establish a list of overdue customers. We consulted with the company data protection officer at a high level over any possible data protection concerns. The DPO identified that our privacy policy might not be worded correctly to allow third party processing and advised to get legal advice. We consulted with Bloggs & Co. Solicitors over the wording of our privacy policy and their advice was that it did in fact allow for third party processing.

We arranged for a meeting with the head of the customer care team and DPO who signed off on....

7. How privacy risks will affect the organisation.

Identify any data protection or privacy risks that may touch upon any governance, compliance or any corporate risks (e.g. potential breach of internal code of conduct, mandatory reporting, etc.)

E.g. The DPO identified that the wording of our privacy policy might not allow for third party processing but we got legal advice from Bloggs & Co. Solicitors who advised that the policy allowed it.

During our assessment, we identified that our antivirus has expired and was not updating with current antivirus protection. We asked IT to renew the antivirus licence, which they did, and we updated our antivirus settings to recues any risk of hacking or accidental data breaches...

Note: you can use the following questions as a guide but they are non-definitive:

- Is there a risk that the security of the personal data can be compromised? If so, how?
- Is there a risk of unauthorised access to the personal data? If so, how?
- Is there a risk that individuals would object to you processing their personal data if they discovered what you were doing? If so, why?
- Is there a risk that the accuracy of the data might not be maintained? If so, how?
- Is there a risk that personal data might be stored or processed longer then is necessary? If so, how?

8. Identify privacy solutions

Describe the actions you took to reduce the risks you identified above, include any action that you must take in order to be compliant (e.g. change wording of application form, update cookie policy, etc.).

If personal data is being transferred outside of the EEA please include the solutions for reducing any privacy risks associated with transferring personal data outside of the EEA.

E.g. We identified a concern over our privacy policy allowing third party processing of personal data but consulted with Bloggs & Co. Solicitors who advised our privacy policy catered for third party transfers of personal data for the purposes of debt collection. IT updated our antivirus to reduce the risk of hacking or accidental damage to data.

Our privacy policy already states that we backup data outside of the EEA and it also explains our secure processes to ensure compliance with GDPR. We have a Data Processing Agreement with a subsidiary in the United Arab Emirates that mandates compliance with EU data protection legislation (GDPR and ePrivacy Directive).

9. Integrate the PIA outcomes (risks identified and solutions) into the project plan.

Identify how the outcomes will be incorporated into the project plan (e.g. updating project documentation, change written processes, etc.), who will do this, who is responsible for implemented the changes, and who is the contact person for any privacy concerns.

Always include a scheduled regular privacy review as part of any changes.

E.g. there is always an ongoing risk of antivirus not being renewed on time so it has now been included in I T systems and processes. As part of this project, any time a privacy review will be carried out it will include ensuring antivirus is valid up to and including the date of the next privacy review.

Etc...

The next scheduled date of privacy review for this project is in three months [Insert date].

10. Sign off and record the PIA outcomes

Identify who has overseen and approved the privacy risks involved in the project. Identify what solutions are yet to be implemented and when will they be implemented.

Please keep this PIA, along with any supporting documentation, on file in accordance with your organisation’s Data Retention Policy.

E.g. This PIA was signed off by [Insert name], [Insert title].

The following solutions have already been implemented:

1. Reviewed policy statements
2. Got legal advice and advised to continue
3. Project documentation was rewritten to include...

The following solutions are yet to be implemented.

1. A privacy review is scheduled in three month's time, on [insert date].
2. Any training relating debt collection going forward will ensure staff are aware of data protection concerns...
...