# GDF Latin America Foundation

# ("The Foundation")

# Data Protection Policy

# Table of contents

# DATA PROTECTION POLICY

## 1. Definitions

| | |
|---|---|
| **Act** | means the Data Protection Act 2017 |
| **Adverse Action** | means any action which may adversely affect the person's rights, benefits, privileges, obligations or interests |
| **Automated data** | means any information on computer, or information recorded with the intention of putting it on computer |
| **Data** | means information in a form which can be processed. It includes both automated data and manual data |
| **Data Controller** | means any person who either alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing |
| **Data Processor** | means any person, other than the data controller, who processes information on behalf of the data controller |
| **Data Protection Officer** | shall be an officer appointed by the Foundation to ensure that the Foundation follows its Data Protection Policy and complies with the Act and the Regulations |
| **Data Protection Policy** | means the present policy |
| **Data Subject** | means an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual |
| **Data Matching Procedure** | means any procedure, whether manually or by means of any electronic or other device, whereby personal data collected for one or more purposes in respect of 10 or more data subjects are compared with personal data collected for any other purpose in respect of those data subjects where the comparison is for the purpose of producing or verifying data, or produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data may be used, whether immediately or at any subsequent time, for the purpose of taking any adverse action against any of those data subjects |

| | |
|---|---|
| **Personal Information** | any information, or opinion forming part of a database which relates to any individual, whose identity is apparent or can be reasonably ascertained from the information or opinion |
| **Processing** | means an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction |
| **Special categories of personal data** | means personal data pertaining to —<br>(a) his racial or ethnic origin;<br>(b) his political opinion or adherence;<br>(c) his religious or philosophical beliefs;<br>(d) his membership of a trade union;<br>(e) his physical or mental health or condition;<br>(f) his sexual orientation, practices or preferences;<br>(g) his genetic data or biometric data uniquely identifying him;<br>(h) the commission or alleged commission of an offence by him;<br>(i) any proceedings for an offence committed or alleged to have been committed by him the disposal of such proceedings or the sentence of any Court in the proceedings |
| **Regulations** | mean the Data Protection Regulations 2009 |
| **Relevant filing system** | means a structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis |

## 1.1 Policy Statement

Fair and lawful treatment of personal information is important for the Foundation as this helps to maintain a high level of confidence and trust in all dealings with the different stakeholders.

To this end, the Foundation endorses and adheres to all the requirements of the Act and the Regulations.

## 1.2 Scope of this Policy

The Act applies to electronic and paper records held in structured filing systems containing personal data. It also applies to personal data held visually in photographs or video clips (including CCTV). As part of its operation, the Foundation collects personal data on various Data Subjects, including information on Beneficiaries, suppliers, Council Members and Founders.

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Act and Regulations.

## 2. Whose rights do the Policy and Act safeguard?

The Act applies to the Foundation's Beneficiaries, Council Members, Founders and any other Data Subject on whom personal information is held and processed.

## 3. Types and Purpose of Data

The Foundation processes data on its Beneficiaries, suppliers, Council Members and Founders. The types of data held and the purpose for processing them in relation to the aforementioned persons are set out in **Annexures I to IV**.

## 4. The Foundation's Responsibilities

In accordance with the Act and Regulations, the Foundation has registered as a data controller on 25th July 2018 with the Mauritius Data Protection Office. The Foundation shall renew the registration every 3 (three) years in accordance with the requirements of the Act.

The Foundation is required to notify the Data Protection Commissioner (DPC) of the types of data it processes on its Beneficiaries, Council Members and Founders. This is included in a public register. The public register on data controllers is available on the DPC's website and at the Data Protection Office.

The Foundation has appointed Abax Corporate Services Ltd (ABAX) as a Data Processor to process the personal data it receives but maintains control by instructing the purposes(s) for which ABAX can process the data.

### 4.1 Data Protection Officer

The Foundation has appointed a Data Protection Officer ('DPO') for monitoring compliance with the Act and Regulations, and for the implementation of this Policy. The Data Protection Officer of the Foundation is Mrs Manisha Padaruth and her responsibilities are as follows:

- Briefing the Meeting of Council Members of the Foundation on the compliance requirements of the Act and data protection best practices;
- Reviewing and updating this Policy;
- Creating and maintaining all relevant documentation required under the Act;
- Act as the main point of contact with the Data Protection Office upon request or voluntarily on data protection issues;
- Reporting any personal data breach to the Data Protection Office within 72 hours;
- Conducting investigation on data breaches to assess the root cause and implement corrective actions;
- Handling subject access requests within 1 month in relation to information held on Beneficiaries, suppliers, Council Members and Founders and liaise with the relevant parties at the Foundation with respect to same;
- Reviewing implications of and giving approval for processing of personal information which are deemed as high risk.

The DPO has the overall responsibility of this Policy. She is responsible for drawing up guidance on good data protection practice and promoting compliance with this Policy and also guidance on how Beneficiaries' personal information are kept, maintained and stored.

The Foundation has put in place the following data protection measures:

### 4.2 Fair collection and processing of data

The Foundation ensures that personal or special categories of personal data are collected lawfully and processes those data fairly. When collecting data, the Foundation shall ensure that the Data Subject concerned is informed of:

- The identity and contact details of the DPO;
- The intended recipients of the data;
- Whether or not the supply of the data by that Data Subject is voluntary or mandatory;
- The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- The existence of the right to request from the Foundation access to and rectification, restriction or erasure of personal data concerning the Data Subject or to object to the processing;
- The existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject;
- The period for which the personal data shall be stored;
- The right to lodge a complaint with the Data Protection Office in Mauritius;
- Where applicable, that the Foundation intends to transfer personal data to another country and on the level of suitable protection afforded by that country; and
- Any further information necessary to guarantee fair processing in respect of the Data Subject's personal data, having regard to the specific circumstances in which the data are collected.

Special categories of personal data shall only be processed in any one of the following conditions:

- The Data Subject has given his express consent;
- The processing is necessary –

  (i) for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject before entering into a contract;

  (ii) for compliance with any legal obligation to which the Foundation is subject;

  (iii) in order to protect the vital interests of the Data Subject;

  (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Foundation;

  (v) the performance of any task carried out by a public authority;

  (vi) the exercise, by any person in the public interest, of any other functions of a public nature;

  (vii) for the legitimate interests pursued by the Foundation or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the Data Subject; or

  (viii) for the purpose of historical, statistical or scientific research.
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the Data Subjects;
- The processing the processing relates to personal data which are manifestly made public by the Data Subject;
- The processing is necessary for –

(i) the establishment, exercise or defence of a legal claim;
(ii) the purpose of carrying out the obligations and exercising specific rights of the Foundation or of the Data Subject; or
(iii) protecting the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving consent.

The Foundation has entered into an addendum to its management/services agreement with ABAX which stipulates that they can only process data pursuant to its engagement and further requires them to comply with equivalent obligations to those imposed on the Data Controller as set out in the Act and Regulations.

### 4.2.1 Subject Consent

Where the processing of data is based on consent, the Foundation will ensure that it is able to demonstrate that the Data Subject has consented to the processing of his or her personal data. The Data Subject consent must be freely given, specific, informed and unambiguous indication of the wishes of the Data Subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.

In cases where it is necessary to obtain consent prior to the processing of data, the Foundation will make the Data Subject aware of its identity and the purposes of the processing for which the personal data is intended and must provide for separate consent to be given for different personal data processing operations where appropriate.

The Foundation shall establish the presence of consent and further demonstrate that:

a) the request for consent was in a concise, intelligible and easily accessible form;
b) where that request was in writing together with other matters, that it was clearly distinguishable from those other matters;
c) where the request for consent was by electronic means, that it was sought in a way that was not unnecessarily disruptive to the use of the service for which the request was provided;
d) where consent was sought for the purposes of the performance of a contract that includes the provision of service that consent was necessary for the performance of the contract or if it was not necessary the Foundation has advised the Data Subject that he or she may refuse separate consent for the provision of the service without prejudice to the performance of the contract;
e) the Data Subject was informed of the right to withdraw consent at any time and that it is as easy to withdraw consent as it was to give it; and
f) the Foundation has taken reasonable efforts to verify that the person giving consent is who the person claims to be.

### 4.2.2 Duty to destroy personal data

Where the purpose of keeping the personal data has lapsed, the Foundation will destroy such data as soon as reasonably practicable, subject to any statutory and administrative requirement or record keeping.

## 4.3 Purpose

The Foundation procures and keeps information for specified and lawful purpose[s] only. This/these purpose [s] will be communicated to the Data Subject prior to requesting the information. A list of the purposes for which the Foundation procures and keeps personal information is listed in **Annexures I to IV**.

Personal information can only be processed in ways compatible with the purposes for which the information was collected. When obtaining personal information for a particular purpose, the data may not be used for any other purpose and personal data may not be divulged to a third party, except in ways that are "compatible" with the specified purpose. Compatibility means whether data is used and disclosed in a way in which those who supplied the information would expect it to be used and disclosed.

## 4.4 Use and further processing of personal information

When processing is for a new or different purpose, the Data Subject should be given the option of saying whether they wish the information to be used in these other ways. **Annexures I to IV** will be amended accordingly.

## 4.5 Right of access to personal data

The Foundation's Beneficiaries, suppliers, Council Members and Founders may request the Foundation to provide them with details and copies of personal information held on them.

The Foundation shall, on the written request of the Data Subject, provide, at at reasonable intervals, without excessive delay and free of charge, confirmation as to whether or not personal data relating to the Data Subject are being processed and forward to him a copy of the data.

The Foundation will respond to Data subject requests electronically where the request was made by electronic means where possible, unless otherwise requested by the Data Subject.

The Foundation may address subject access requests by the use of the Subject Access Request Form in **Appendix A**.

The Foundation may restrict access to personal data in the following circumstances:

- Where the Foundation is not supplied with the information it reasonably requires in order to satisfy itself as to the identity of the person making the request and to locate the information which the person seeks;
- Where compliance with the request would be in contravention of the confidentiality obligation of the Foundation under the Mauritian law;
- The right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person. Where personal data consists of expressions of opinion about the data subject by another person, the Data Subject has a right to that expression of opinion except where that expression of opinion was given in confidence;
- Where the Foundation cannot comply with the request without disclosing personal data relating to another person, it may refuse the request unless the other individual has consented to the disclosure of his personal data to the person making the request or he obtains the written approval of the DPC;
- Where there is a revelation of evidence of the commission of a criminal offence by the Foundation other than an offence under the Act.

### 4.6 Right to be forgotten

The Foundation will comply with requests from Data Subjects for the erasure of their personal data without undue delay where doing so would not contravene any operational, legal or regulatory requirements under which the Foundation operates.

Upon receipt of a request for the erasure of a Data Subject's personal data, the Foundation will adhere to the request without undue delay where the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed and there is no legal or regulatory requirement to hold the data.

The Foundation will address the Data Subject's right to be forgotten by the use of the Right to Erasure Request form in **Appendix B**.

### 4.7 Right to Rectification

The Foundation will comply with requests from Data Subjects for the rectification of data held on them in a timely manner.

Upon receipt of a written request from a Data Subject confirming that the data held is inaccurate or incomplete, the Foundation will:

a) take all reasonable steps to confirm that the personal data is inaccurate or incomplete and to rectify or complete the data;
b) take no action where the Foundation determines that it is satisfied as to the accuracy and completeness of the personal data;

c) where is it unreasonable to confirm or verify the accuracy of the personal data, the Foundation will record a statement in respect of that personal data that confirms that the Data Subject has disputed the accuracy or completeness of that personal data.

The Foundation will address the Data Subject's right to rectification by the use of the Right to Rectification Request form in **Appendix C**.

### 4.8 Right to Restrict Processing

In the circumstances where a Data Subject has a right to restrict the processing undertaken, and upon receipt of such a request, the Foundation will restrict all processing in accordance with the Act.

Data Subjects have the right to restrict processing where one of the following circumstances applies:

a) where the accuracy of the personal data is contested by the Data Subject, for such a period as will enable the Foundation to verify the accuracy of the personal data;
b) where the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of its use instead;
c) where the Foundation no longer needs the personal data for the purpose of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
d) where the Data Subject has objected to processing which has been undertaken exclusively on reasons of public function and/or legitimate interests (i.e. where there is no contract, consent or vital interests to require the processing) until such time as the public function and/or legitimate interests of the Foundation override those of the Data Subject.

Where a restriction has been put in place in satisfaction of one of the above conditions and that restriction is to be lifted the Foundation will write to the Data Subject to inform them of the same before lifting the restriction.

Where data processing has been restricted, the personal data affected, with the exception of storage, may only be processed in the following situations:

a) with the Data Subject's consent;
b) for the purposes of any legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights;
c) where it is necessary in order to protect the vital interest of the Data Subject or any natural person;
d) where the processing is necessary for reasons of substantial public interest provided for by law and is subject to appropriate protections to protect the rights and interests of the Data Subject.

The Foundation will address the Data Subject's right to restrict processing by the use of the Right to Restrict Processing Request form in **Appendix D**.

### 4.9 Accurate and Up-to-date data

The Foundation takes reasonable steps to ensure that personal information is accurate and up to date.

All Beneficiaries shall:

- Ensure that all personal information which they provide to the Foundation is accurate and up to date;
- Inform the Foundation of any changes to the information provided above without undue delay;
- Check the information which the Foundation shall make available from time to time, in written or automated form, and inform the Foundation of any errors therein. The Foundation shall not be held responsible for errors of which it has not been informed;

### 4.10 Adequate, relevant and not excessive

When collecting or keeping personal information, the Foundation shall ensure that it is just and commensurate to its purpose. Information not needed should not be sought for.

### 4.11 Security of personal data

The Foundation has put appropriate security and organisational measures in place to prevent unauthorised access to, alteration of, disclosure of, accidental loss, and destruction of the data in its control. Personal information is kept in a safe and secure place, especially confidential and sensitive information.

The Foundation reviews its security measures on a regular basis to ensure that they are up to date and effective and also to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

The Foundation has also put in place a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

As regards transmission of personal data over a network, the Foundation has put in place measures such as IT security, back up, firewalls, virus protection, password protection to computer terminals, and restricted access to information on a need-to-know basis.

The Foundation has taken the following measures to prevent the unauthorised destruction or alteration of:

- The pseudonymisation and encryption of personal data;
- Access to information has been restricted on a "need-to-know" basis;
- Computer systems containing personal data are password protected;
- A Sophos total protection has been installed on all computers;
- Back-up procedure, including off-site back-up in order to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Waste papers and printouts containing personal information are shredded;

### 4.12 Retention of personal data

The Foundation shall keep the different types of information for differing length of time depending on legal and operational requirements.

Information no longer required shall be disposed of appropriately.

### 4.13 Disclosure of personal data

Strict conditions apply to the passing of personal information both internally and externally. The Foundation shall not disclose personal information to any third party unless it is lawful to do so.

Circumstances where disclosure of data is required and necessary:

- Under any enactment or by a Court order;
- For the purpose of, or in connection with, any on-going or prospective legal proceedings;
- For the purpose of obtaining legal advice; or
- For the purpose of establishing, exercising or defending legal rights.

### 4.14 Record of processing operations

The Foundation shall maintain a record of all processing operations. The record shall set out the following:

- The name and contact details of the Data Processor, and, where applicable, his or its representative and the data protection officer;
- The purpose of the processing;
- A description of the categories of data subjects and of personal data;
- A description of the categories of recipients to whom personal data have been or will be disclosed, including recipients in other countries;
- Any transfers of data to another country, and the suitable safeguards;
- Where possible, the envisaged time limits for the erasure of the different categories of data; and
- The description of the relevant policies and mechanisms in place.

## 4.15 Data protection impact assessment

Where processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature scope, context and purposes the Foundation, shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

## 4.16 Transfers abroad

The Foundation may transfer personal data to another country where –

- it has exercised appropriate safeguards with respect to the protection of the personal data;
- the Data Subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards;
- the transfer is necessary –

    (i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
    (ii) for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Foundation and another person;
    (iii) for reasons of public interest as provided by law;
    (iii) for the establishment, exercise or defence of a legal claim; or
    (iv) in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent; or
    (v) for the purpose of compelling legitimate interests pursued by the Foundation which are not overridden by the interests, rights and freedoms of the data subjects involved and where –

        (A) the transfer is not repetitive and concerns a limited number of data subjects; and

        (B) the Foundation has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Data Protection Office in Mauritius proof of appropriate safeguards with respect to the protection of the personal data; or

- the transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that

the conditions laid down by law for consultation are fulfilled in the particular case.

### 4.17 Direct Marketing

The Act applies to all forms of direct marketing which is defined as the communication of any advertising or marketing material which is directed to any particular individual. No one should receive unsolicited direct marketing of any nature unless he has indicated that he consents, or at least that he does not object, to such uses of his personal data. Consent needs not be in writing for direct marketing purposes and can be implied in certain circumstances.

Personal information obtained in the past cannot be used for a different purpose or personal data cannot be sold for direct marketing purposes unless consent of all the individuals affected to this use of their personal data has been given.

Direct marketing should not be targeted at people referred by existing customers unless an individual has, in his own right, given his clear consent to receive direct marketing correspondences.

### 4.18 Data Matching

The Foundation does not currently carry out data matching procedure. It shall carry out data matching procedure only when the individual and the DPC have consented and where the DPC has imposed any conditions for the carrying out of the procedure or when the procedure is required by law.

The Foundation shall not take any adverse action against any Data subject as a consequence of the carrying out of a data matching procedure unless the Foundation serves a notice in writing on the data subject specifying the adverse action it proposes to take and the reasons for so doing and further stating that the data controller has 7 days after the receipt of the notice to say why the adverse action should not be taken.

## 5. Breach Reporting

It is the policy of the Foundation to maintain a register of data breaches and in the case of a Personal Data Breach, the Foundation shall, without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, notify the Data Protection Office in Mauritius, in writing, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The Foundation will maintain a register of data breaches that will include in as much detail as possible the facts relating to the Personal Data Breach, its effects and the remedial action taken.

As soon as practicable and no later than 72 hours following the discovery of a Personal Data Breach, the Foundation is required to write to the Data Protection Office in Mauritius in clear and plain language providing:

a) a description of the nature of the Personal Data Breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) the name and contact details of the contact point where further information can be obtained;
c) an overview of the likely consequences of the Personal Data Breach; and
d) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including where appropriate, measures to mitigate its possible adverse effects.

The data breach will not be communicated to the Data Protection Office in Mauritius if:

a) the Data Controller has implemented proportionate technical and organisational protection measures, and those measures were applied to the personal data affected by the Personal Data Breach, in particular measures that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the Data Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is unlikely to materialise;
c) it would involve disproportionate effort, in which case there must be a communication or similar measure whereby the data subjects are informed in an equally effective manner.

Where the data breach is likely to result in a high risk to the rights and freedoms of individuals, the Foundation must also communicate the Personal Data Breach to the Data Subject without undue delay.

The Foundation will address data breaches by the use of the Data Breach Notification Form in **Appendix E**. When assessing the severity of the risk associated with the breach, it may use the Risk Assessment in **Appendix F**.

## 6. Compliance with this Policy

Compliance with this Policy and this Act is the responsibility of all the Council Members.

Any individual who considers that the Policy has not been followed in respect of personal data about himself/herself should raise the matter with the DPO.

## 7. Effective Date

This Policy is effective as of 11th October 2018.

## ANNEX I: Types and Purpose of data held on individual Beneficiaries

| Types of Data | Purpose |
|---|---|
| • Name;<br>• Residential address;<br>• Proof of residential address;<br>• Telephone and mobile number;<br>• ID and Passport copies;<br>• Bank Reference letter;<br>• Banking details;<br>• CV;<br>• Email address;<br>• Bank account number; and | (i) Legal and regulatory requirements<br>(ii) Provision of corporate advisory and administration services; and<br>(iii) Statutory record keeping |

## ANNEX II: Types and Purpose of data held on any parties related to the day to day operations of the Foundation

| Types of Data | Purpose |
|---|---|
| • Name;<br>• Business address;<br>• Business telephone and mobile number; and<br>• Business email address | (i) Payment purposes<br>(ii) Purchase/order requirements<br>(iii) Know-your-client |

## ANNEX III: Types and Purpose of data held on Council Members and Founders

| Types of Data | Purpose |
|---|---|
| • Name;<br>• Residential address;<br>• Proof of residential address;<br>• Telephone and mobile number;<br>• ID and Passport copies;<br>• Bank Reference letter;<br>• Bank account number;<br>• CVs;<br>• Email address;<br>• Bank account number; and | (i) Regulatory requirements<br>(ii) Registry<br>(iii) Statutory record keeping |

# Appendix A

## *Subject Access Request Form*

| | | | |
|---|---|---|---|
| **Completion by Council Member** | | | |
| **Data Controller** | | | |
| **Data Subject Type i.e. Shareholder/ Council Member** | | | |
| **Data Subject Name** | | | |
| **Date Subject Access Request (SAR) received and by whom** | | | |
| **Method of receipt** | | | |
| **Mandatory Response Date (Mandatory for information to be provided within one month from receipt of request)** | | | |
| **Has the Data Subject been adequately identified? Please give details.** | | | |
| **Date SAR passed to Data Protection Officer(DPO)** | **Date:** | | |
| **Completion by Data Protection Officer** | | | |
| **Is the Data Subject permitted to obtain the requested information or has appropriate authorisation been given for a third party to act on behalf of the Data Subject? Please give details.** | | | |
| **Details of specific data requested or "All" (If not "All", please itemise)** | | | |
| **Is data request considered to be "manifestly unfounded or excessive?" (i.e. repetitive) (Please circle)** | **Yes/ No** | **If yes, action taken** | |
| **Is it likely that an extension will be required to the standard one month response time in order to provide the requested data?** | **Yes/ No** | **If yes, action taken (including advising data subject)** | |
| **Is there a need to consider legal advice?** | **Yes/ No** | **If yes, action taken** | |
| **Independent check performed to ensure only Data Subject** | **Check performed by:** | **Job Title:** | **Signature:** |

| | | | |
|---|---|---|---|
| **information is disclosed. Any other data must be anonymised prior to sending.** | | | |
| **Method that data will be provided to Data Subject (Please circle)** | • **Electronic Format**<br>• **By Post**<br>• **Collect the information in person**<br>• **Letter detailing only types of data held rather than copies of the information**<br>• **Other method, as requested by the Data Subject i.e. view a copy of the information only** | | |
| **Date Paper information received by/DPO** | | | |
| **Date Electronic information received by DPO** | | | |
| **Personal Data Schedule (see below) completed** | **Date** | | |
| **Date response to Data Subject sent** | | | |
| **Added to SAR Register** | | | |
| | | | |
| **Copy of all information provided scanned and saved together with covering letter/email** | | | |
| **Details/Comments** | | | |

| **Name** | **Signature** | **Date** |
|---|---|---|
| **Data Protection Officer** | | |
| **Council Member** | | |

# Appendix B

## *Right to Rectification Request*

| **Completion by Council Member** | | |
|---|---|---|
| Data Controller Name | | |
| Client Number | | |
| Date request received and by whom | | |
| Method of receipt | | |
| Mandatory Response Date (Mandatory for information to be provided within one month from receipt of request) | | |
| Is the request for rectification valid and has adequate identification taken place? | **Details:** | |
| Date request passed to Data Protection Officer (DPO) | | |
| **Completion by Data Protection Officer** | | |
| Details of rectification requested | | |
| If the personal data in question has been disclosed to others, you must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. | **Yes/ No** | **Details:** |
| Where a decision is reached to take no action, an explanation must be provided to the individual, stating the reason such decision was reached and informing them of their right to complain to a supervisory authority and to a judicial remedy | **Details:** | |
| Is it likely that an extension will be required to the standard one month response time in order to rectify the data? | **Yes/ No** | **If yes, reason for extension and action taken (including advising data subject)** |
| Request passed for rectification of records. | | |
| Confirmation received that information has been rectified in line with request. | | |
| Details/ comments | | |

| **Name** | **Signature** | **Date** |
|---|---|---|
| **Data Protection Officer** | | |
| **Council Member** | | |

# Appendix C

## *Right to Erasure Request*

| **Completion by Council Member** | | |
|---|---|---|
| Data Controller Name | | |
| Client Number | | |
| Date request received and by whom | | |
| Method of receipt | | |
| Mandatory Response Date<br>(Mandatory response within one month from receipt of request) | | |
| Has adequate identification taken place? | **Details:** | |
| Date request passed to Data Protection Officer | | |
| **Completion by Data Protection Officer** | | |
| Reason for erasure request | • The personal data is no longer necessary in relation to the purpose for which it was originally collected/ processed.<br>• The individual withdraws consent.<br>• The individual objects to the processing and there is no overriding legitimate interest for continuing the processing.<br>• The personal data was unlawfully processed (ie otherwise in breach of the Act).<br>• The personal data has to be erased in order to comply with a legal obligation.<br>• The personal data is processed in relation to the offer of information society services to a child. | |
| Is the request deemed valid and will it be complied with? If No see below | **Yes/ No** | |
| If the personal data in question has been disclosed to others, you must contact each recipient and inform them of the erasure - unless this proves impossible or involves disproportionate effort. | **Yes/ No** | **Details:** |
| Reason Request for Erasure denied<br>*Where you are not taking action in response to a Request for Erasure, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.* | • to exercise the right of freedom of expression and information;<br>• to comply with a legal obligation for the performance of a public interest task or exercise of official authority.<br>• for public health purposes in the public interest;<br>• archiving purposes in the public interest, scientific research historical research or statistical purposes; or<br>• the exercise or defence of legal claims. | |

| | | |
|---|---|---|
| | **Details:** | |
| Is it likely that an extension will be required to the standard one month response time in order to erase the data? | **Yes/ No** | **If yes, reason for extension and action taken (including advising data subject)** |
| Confirmation to Council Member that data has been erased. | | |
| Copy of supporting documents and covering letter to client scanned and saved | | |
| Details/ comments | | |

| **Name** | **Signature** | **Date** |
|---|---|---|
| **Data Protection Officer** | | |
| **Council Member** | | |

# Appendix D

## *Right to Restrict Processing Request*

| **Completion by Council Member** | | |
|---|---|---|
| Data Controller Name | | |
| Client Number | | |
| Date request received and by whom | | |
| Method of receipt | | |
| Mandatory Response Date (Mandatory for response to be provided within one month from receipt of request) | | |
| Is the Restrict Processing request valid and has adequate identification taken place? | **Details:** | |
| Date request passed to Data Protection Officer | | |
| **Completion by Data Protection Officer** | | |
| Reason for Restrict Processing Request | • An individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.<br>• Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or for legitimate interests), and consideration needs to be given to whether the legitimate grounds override those of the individual.<br>• When processing is unlawful and the individual opposes erasure and requests restriction instead.<br>• If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim. | |
| Is the request valid and will it be complied with?<br><br>Where you are not taking action in response to a Request to Restrict Processing, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy. | **Yes/ No** | **If No reason for request denied:** |
| If the personal data in question has been disclosed to others, you must contact each recipient and inform them of the restriction - unless this proves impossible or involves disproportionate effort. | **Yes/ No** | **Details:** |
| Is it likely that an extension will be | **Yes/** | **If yes, reason for extension and action** |

| | | |
|---|---|---|
| required to the standard one month response time in order to restrict the data? | **No** | **taken (including advising data subject)** |
| Confirmation to Council Member that Request to Restrict Processing has been complied with. | | |
| Copy of supporting documents and covering letter to client scanned and saved | | |
| Details/ comments<br>(You must inform individuals when you decide to lift a restriction on processing). | | |

| **Name** | **Signature** | **Date** |
|---|---|---|
| **Data Protection Officer** | | |
| **Council Member** | | |

# Appendix E

## *Data Breach Notification Form*

| | | |
|---|---|---|
| Is Personal Data involved? | Yes/ No | |
| Data Controller Name | | |
| Client Number(s) | | |
| Date and time incident occurred and how you became aware | | |
| Details of the incident | | |
| Type of breach<br>(please circle accordingly) | Confidentiality Breach<br>(an unauthorised or accidental disclosure of, or access to, personal data)<br><br>Integrity Breach<br>(an unauthorised or accidental alteration of personal data)<br><br>Availability Breach<br>(an unauthorised or accidental loss of access to, or destruction of, personal data) | |
| Date and time initial notification made via telephone to the Data Protection Officer. | | |
| **Completion by Data Protection Officer** | | |
| If Personal Data is involved Risk Assessment undertaken<br>(see below) | Outcome: | |
| Is there any risk to rights and freedoms of individuals?<br>(If Yes, notification to supervisory authorities to be made within 72 hours) | Yes/ No | Date and details of notification(s) made: |
| Is the risk to the rights and freedoms of individuals assessed to be high?<br>(If Yes, notification to relevant individuals to be made without undue delay) | Yes/ No | Date and details of notification(s) made: |
| | | |

| | |
|---|---|
| Outcome of investigation | |
| Mitigating action(s) identified to prevent a recurrence | |
| Responsibility to implement mitigating action(s) and target date | |

| **Name** | **Signature** | **Date** |
|---|---|---|
| **Data Protection Officer** | | |

# Appendix F

## *Risk Assessment*

It is necessary to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring.
In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

| **Completion by Data Protection Officer** | | | |
|---|---|---|---|
| Client Name (Data Controller) | | | |
| Fund (if applicable): | | | |
| Is Personal Data Involved | Yes/ No | If Yes, type of data (i.e. was sensitive data involved?) | |
| Potential adverse effects | • Loss of control over individuals personal data<br>• Limitation of individuals rights<br>• Discrimination<br>• Identity theft or fraud<br>• Financial Loss<br>• Unauthorised reversal of pseudonymisation<br>• Damage to reputation<br>• Loss of confidentiality of data protected by professional secrecy<br>• Any other significant economic or social disadvantage to the natural person concerned. | | |
| Was the data encrypted? | Yes/ No | Details: | |
| The nature/ sensitivity and volume of personal data/ the combination of personal data | | | |
| Ease of identification of individuals | | | |
| Severity of consequences for individuals | | | |
| Number of individuals affected | | | |
| Is there any risk to rights and freedoms of individuals?<br>(If Yes, notification to supervisory authorities to be made within 72 hours) | Yes/ No | Justification: | |
| Is the risk to the rights and freedoms of individuals assessed to be high?<br>(If Yes, notification to relevant individuals to be made without undue delay) | Yes/ No | Justification: | |
| **Name** | | **Signature** | **Date** |
| **Data Protection Officer** | | | |