Caribbean Regional Fisheries Mechanism (CRFM)

Personal Data Protection Policy 2022

Table of Contents

1.0 BACKGROUND, PURPOSE AND SCOPE

1.1 Privacy of the individual has been recognised as a human right, as enunciated in international instruments such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the American Convention on Human Rights, and the European Convention on Human Rights. The right to privacy protects the individual's private life against arbitrary, unlawful or abusive interference. It provides for the protection of the personal information of the individual, and the protection of the transmission of such information.

1.2 Privacy and Data Protection laws have been widely enacted globally and in the Caribbean region in recent years to regulate the collection, keeping, use and dissemination of personal data and to protect the privacy of individuals in relation to their personal data. These laws are based on the premise that the individual must have some level of control over how the personal information collected from them, whether by the government, businesses, international and regional organisations is utilised, processed or disclosed.

1.3 The CRFM Personal Data Protection Policy (hereinafter referred to as the 'Policy') was developed in accordance with the current global normative framework, international best practices and standards, and CARICOM's policy on personal data protection and processing, with a view to strengthening institutional control mechanisms and fostering transparent and proper use of the personal data of employees and individuals collaborating with the CRFM to fulfill its mission.

1.4 The purpose of the Policy is to ensure that the roles and responsibilities of employees of the CRFM Secretariat with respect to protecting personal data are clearly defined, understood, and followed by all employees. The document also provides procedural guidance on how the CRFM Secretariat, and its governance bodies will implement the Policy.

1.5 This Policy applies to all individuals who have a direct involvement with the CRFM Secretariat including consultants, interns, suppliers, contractors, Members and Advisors of the Ministerial Council, Caribbean Fisheries Forum, Executive Committee, Sub-committees, and Working Groups; counterparts and strategic partners, donors, among others, in all Member States and at Headquarters, with whom the CRFM is collaborating to fulfill its mission.

1.6 The Policy and procedures are applicable to all areas of work of the CRFM and sets out the requirements, standards and expectations for the protection of Personal Data relating to an identifiable Data Subject.

2.0 DEFINITIONS

Contractors – This includes individuals who are independent contractors, consultants, interns or contingent workers.

Data – means Information that is either processed by or intended to be processed by, in response to instructions given for that purpose; or information that is recorded as part of, or with the

intention of forming part of, a "relevant filing system" of information that forms part of an accessible record of the CRFM. Data includes any document, correspondence, memorandum, book, plan, map, drawing, pictoral or graphic work, photograph, film, microfilm, sound recording, videotape, machine-readable record and any other documentary material, regardless of form or characteristics, and any copy of those things.

Data Controller – A person or organisation that makes decisions regarding the Personal Data to be processed. The Data Controller decides the purpose for which Personal Data is to be processed, what Personal Data is required and how it is obtained.

Data Protection - The fair and proper use of information about people. It is part of the fundamental right to privacy.

Data Protection Officer (DPO) – The Data Protection Officer is responsible for the oversight, development and maintenance of all data protection and privacy functions within the CRFM Secretariat. The DPO ensures compliance with all applicable laws and regulations and with this policy.

Data Protection Event – Any situation, whether suspected or proven, deliberate or inadvertent, that exposes the Personal Data of a Data Subject to unauthorised individuals.

Data Processor – A Data Processor is any person (other than an employee of the Data Controller) that processes Personal Data on behalf of the Data Controller.

Data Subject – A living individual to whom data relates and whose data will be subject to processing. Data Subject include, but are not limited to, Employees, contractors, consultants, donors, development partners, fishers, interns, and implementing partners.

Employees – means current and former employees of the CRFM Secretariat.

Personal Data – means information about an identifiable individual that is recorded in any form including—

(a) information relating to the nationality, address, age, contact details, country of residence, fax numbers, postal numbers or marital status of the individual;
(b) information relating to social security status, national insurance contributions and judicial records of the individual;
(c) any information supplied as information and evidence by an individual pursuant to the CRFM Secretariat's Operations Manual;
(d) information supplied pursuant to the disposal of assets procedure by the Secretariat;
(e) information on the racial or ethnic origins of the individual[1];
(f) information on the political opinions or affiliations of the individual; information on religious beliefs or other beliefs of a similar nature of the individual[2];
(g) information relating to physical or mental health or condition of the individual;

[1] The CRFM Secretariat does not request the type of information described in (e), (f) and (i), but is not oblivious, that notwithstanding same, said information may come into its possession.
[2] Ibid

(h) information related to fingerprints, deoxyribonucleic acid, blood type or bio-metrics of the individual;
(i) information related to the sexual orientation or sexual life of the individual[3]
(j) information related to the criminal or financial record of the individual;
(k) information relating to the education, technical skills, expertise, languages, professional experience or employment history of the individual;
(l) information supplied by an individual pursuant to employment opportunities, including the personal information of references, birth certificates, medical records, passport information, photographs, banking data, and information concerning a spouse, children or other dependants of the individual;
(m) any identifying number, symbol or other particular designed to identify the individual;
(n) the views and opinions of any other person about the individual;
(o) The terms of any lease agreements entered into by employees of the Secretariat;
(p) correspondence sent to an establishment by the individual that is explicitly or implicitly of a private or confidential nature, and any replies to such correspondence which would reveal the contents of the original correspondence;

Sensitive Personal Data – means personal Data of the Data Subject consisting of information as to their racial or ethnic origins, political opinions, religious beliefs, trade union membership, physical and mental health (including disabilities), sexual life, the commission or alleged commission of any offence and any legal proceedings (including the disposal of legal proceedings) or any court sentence in connection with any offence committed or alleged to have been committed by the Data Subject.

Processing - in relation to information or data means obtaining, recording, or holding the information or data and any operation performed on the information or data such as viewing, amending, sharing, deleting, or storing or any other use that might be done to or with the data.

Data Subject Access Requests – means Data Subject rights to information about the Personal Data relating to them which is in the control of the Data Controller.

Legitimate Interest - Interest of the Data Controller or of Third Parties that justifies the processing of the Personal Data, without the consent of the Data Subject, provided that the necessary consideration has been given to the Data Subject's rights and interests, fundamentally, the right to a private life and to personal data protection.

Third Party - means any individual or legal person other than the data subject or the CRFM. Some examples of third parties are regional institutions, national or local governments, consultants, as well as development partners or allies, whether public or private.

[3] Ibid

3.0 ROLES AND RESPONSIBILITIES

3.1 All Employees, consultants, interns and contractors of the CRFM Secretariat managing and handling Personal Data need to understand their responsibility for good data protection practice and must follow the procedures outlined below. They must:

(i) Be aware of this policy and comply with it.
(ii) Understand which information they have the right of access to.
(iii) Know the information for which they are owners.
(iv) Know the information systems and computer hardware for which they are responsible.

4.0 GOVERNANCE

4.1 The Executive Director of the CRFM (hereinafter referred to as 'the Executive Director) shall be the Data Protection Officer and shall have overall responsibility for the production, maintenance and communication of this policy document and any sub-policy documents or guidelines developed thereunder.

4.2 The Executive Director of the CRFM may delegate the functions of the Data Protection Officer including the day-to-day implementation of this Policy to any member of the Senior management team such as the Deputy Executive Director or the Manager, Finance and Administration or a Programme Manager.

4.3 The CRFM Personal Data Protection Policy shall be reviewed regularly and kept up to date in accordance with relevant policies of Caribbean Community and international best practice and procedures.

4.4 It is the responsibility of the Executive Director to ensure that these reviews take place.

4.5 Any substantive changes made to the Policy will be reviewed and approved by the established decision-making process of the CRFM and communicated to all relevant personnel.

5.0 CRFM EMPLOYEES

5.1 When a new Employee joins the CRFM Secretariat they must undertake the induction training which will include data protection training. This training must be completed within the required timeframe.

5.2 All current employees of the CRFM will receive ongoing data protection training where required. It is the responsibility of each employee to familiarize themselves with the content of the policy

5.3 All employees are required to follow these policies, procedures and standards, and any further amendments or guidelines issued in connection with them.

6.0 PROGRAMME MANAGERS AND SUPERVISORS

6.1 Programme Managers and Supervisors must ensure that everyone managing and handling Personal Data is appropriately trained to do so and that everyone managing and handling Personal Data is appropriately supervised.

6.2 At the local level, the Programme Manager is responsible for ensuring that:

6.3 These procedures and standards and any further guidelines are followed.

6.4 These procedures and standards are fully implemented within their section or unit.

7.0 OVERALL RESPONSIBILITIES – DATA PROTECTION OFFICER (DPO)

7.1 The role of the DPO is to:

(i) Oversee organisation's compliance with the Data Protection Policy and any other applicable international standards or statutory requirements in jurisdiction in which the CRFM operates.

(ii) Ensure that procedures and standards regarding the processing of Personal Data are compliant with this Policy and implemented.

(iii) Oversee responses to subject access requests

(iv) Ensure relevant data protection / privacy notices are used and relevant consents are obtained

(v) Investigate and track any breaches in Data Protection Policy and report to the members of the Forum or Executive Committee

(vi) Promote training and awareness.

(vii) Oversee regular monitoring of Data Protection issues.

(viii) Conduct ad hoc reviews where required.

(ix) Provide guidance and answer any Data Protection queries from the business where required.

(x) Ensure Data Protection Impact Assessments (DPIA) or other appropriate assessments are carried out where required.

(xi) Should there be any issues that cannot be resolved locally the Programme Manager or Supervisor should contact the Executive Director. The use of these procedures and standards and any further guidelines may be audited from time to time by the Executive Director / DPO, as well as, by external auditors

8.0 PROCESSING PERSONAL DATA FAIRLY AND LAWFULLY

(i) The CRFM Secretariat holds personal Data about a Data Subject that is sufficient for the purpose it is being held in relation to that Data Subject, and The CRFM Secretariat does not hold more information than needed for that purpose. The minimum amount of Personal Data needed to fulfil the purpose for processing should be identified. Only this information should be held and no more.

(ii) Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
(iii) Internal data sharing requests within the CRFM should be reviewed by the Executive Director for reasonableness with the focus being on limiting the amount of Employee, Customer, contractor Personal Data shared.
(iv) Employees must ensure any transmissions of data outside the CRFM Secretariat are referred to the Executive Director when there is no operating agreement already in existence between the CRFM and the outside entity.
(v) When sharing or transmitting data outside the CRFM the least amount of Personal Data necessary to fulfil the operational need should be transmitted.
(vi) The Executive Director may require a risk assessment prior to sharing the data by completing a Data Privacy Impact Assessment (DPIA) and approve the Personal Data items.

8.1 Privacy Notices

Privacy Notices must adequately describe:
(i) The CRFM Secretariat as the Data Controller.
(ii) Why the Personal Data is collected and how The CRFM Secretariat intends to use the Personal Data collected about the Data Subject.
(iii) If the CRFM Secretariat intends to share the Personal Data and who it will be shared with.
(iv) The types of information collected constituting Personal Data and the methods of collection.
(v) All privacy notices must be reviewed and approved by the Executive Director
(vi) Privacy notices are updated when there are updates to these procedures and standards or operational practice.

8.2 Use of personal information

8.2.1 Personal data held by the CRFM Secretariat will be included in a database or physical repository and may be used for the following purposes:
(i) to meet the objectives of contractual relationships;
(ii) to contact the Data Subject and respond to any request he or she may have sent via the CRFM's knowledge management system (websites, email, facebook etc.);
(iii) to share informational material and publications of the CRFM, in keeping with the Data Subjects' interests;
(iv) to conduct surveys among stakeholders;
(v) to address requests, complaints or claims that the Data Subject has a right to make as a person that utilizes CRFM's information services;
(vi) to manage and reply to comments or requests made through press releases or other communication issued by the CRFM Secretariat, which are open for participation by the Data Subject;
(vii) to compile general statistics; and
(viii) to make any other lawful, fair, just and transparent use within the scope of CRFM's mandate and activity.

8.2.2 The CRFM uses cookies that store general, non-personal information to measure the number of visits to our sites, the average time spent on the site, pages visited, and other similar information, and to improve content and ensure security and protection of data.

8.2.3 The CRFM does not release, rent, allocate, transfer nor provide personal information to third parties without prior consent of the Data Subject, except when:

(i) it is general public knowledge at the moment it is divulged or it becomes public domain through no illegal action on the part of the CRFM;
(ii) it is in the possession of the CRFM at the moment it is divulged, without the CRFM violating any legal obligation or the objective of this Policy;
(iii) it becomes known to the CRFM from a third-party source (i.e. not the Data Subject), but with the legal right to divulge such Personal Information; or
(iv) it must be divulged by the CRFM in order to comply with applicable government laws or regulations.

8.3 Personal Data must be processed fairly and lawfully

In practice, it means the following:

(i) Legitimate grounds must exist for collecting and using the Personal Data. Particular care has to be given in relation to the processing of Sensitive Personal Data;
(ii) Sensitive Personal Data can only be processed with the explicit consent of the Data Subject and must be kept secure at all times.
(iii) In instances where it is suspected that a data subject may be suffering from a mental health condition, or be classed as vulnerable, by way of age, disability or otherwise advice should be sought from the Executive Director, or the mental health subject matter experts.

8.4 Personal Data should not be used in ways that have unjust adverse effects on the Data Subjects

(i) Data Subjects should be provided with appropriate privacy notices when their personal data is being collected to ensure transparency about the intended use of their Personal Data.
(ii) Personal Data should only be handled in ways they would reasonably expect.
(iii) The personal data should not be used in any unlawful way or for any unlawful purpose
(iv) New or changed methods of collecting Personal Data must be reviewed by the Executive Director before they are implemented to confirm that Personal Data is obtained fairly and lawfully. This may be done by a risk assessment utilising an appropriate Data Privacy Impact Assessment Form (DPIA)

8.5 Keeping Personal Data accurate and up to date

8.5.1 The CRFM Secretariat must make every effort to ensure the accuracy of any Personal Data obtained and ensure that the source of any Personal Data is clear, carefully consider any

challenges to the accuracy of information and consider whether it is necessary to update the information.

8.5.2 The CRFM Secretariat must inform Data Subjects that they have the right to amend or delete incorrect data in the privacy notices provided to Employees and customers.

8.5.3 The CRFM Secretariat should contractually obliges Data Subjects who are its employees, contractors, customers to notify it of any changes in their details.

8.5.4 The CRFM Secretariat will perform data quality reviews on *an ad* hoc basis or when required to ensure that the data managed or processed is accurate and up to date. This includes reviews, data integrity controls and process review.

8.6 Security and integrity of the data

8.6.1 The CRFM Secretariat will take reasonable security measures against risks to data provided, such as unauthorised access, changes, retention, use, disclosure and disposal of information. The information provided by a Data Subject will be stored and protected in keeping with industry and technology standards. However, the internet is not a space that is 100% secure; therefore, CRFM cannot guarantee that transmissions via the Internet will be completely private or secure.

8.6.2 Data Subject understand that any message or information sent to the CRFM can be intercepted or read by Third Parties, even when the information is encrypted. Therefore, a data subject agrees to hold the CRFM harmless from any liability.

8.7 Retaining Personal Data

8.7.1 The CRFM Secretariat must review the length of time the Personal Data is kept. The CRFM Secretariat should consider the purpose or purposes for holding the information when deciding whether (and for how long) to retain it.

8.7.2 The CRFM Secretariat can retain data provided by a Data Subject so long as to ensure that the Data Subject has a reasonable opportunity to obtain access to said information.

8.7.2 The CRFM Secretariat must securely delete information that is no longer needed for this purpose or these purposes and update, archive or securely delete information if it becomes out of date.

9.0 RIGHTS OF THE DATA SUBJECT

Personal Data shall be processed in accordance with the rights of Data Subjects under the Policy. The rights of the Data Subject are:

Right of access – Data subjects have a right to access to their data and to certain information about the processing of that personal data. This information must usually be provided free of charge within a month of receiving a request from the Data Subject.

Right of rectification (correction) – The Data Subject has the right to ask for his or her personal data to be corrected if it is inaccurate and completed if it is incomplete.

Right to have personal data erased of "Right to be forgotten" – in certain circumstances a Data Subject can ask the CRFM to erase his or her personal data. It may not be possible to accept a Data Subject request if, for example, the CRFM has a contractual or other legal duty to retain the information.

Right to restriction of processing – in certain circumstances Data Subjects have a right to restrict or object to the processing of their personal data when it is being processed on the basis of CRFM's legitimate interest. This may include when the Data Subject disputes its accuracy (until the accuracy is proved); if a Data Subject has objected to the processing (when it was necessary for the legitimate interest of the CRFM) and the CRFM is considering whether its legitimate interest overrides the interest of the Data Subject; or if the CRFM no longer needs the data but the Data Subject want the CRFM to keep it in order to establish, exercise or defend a legal claim. Data Subjects have an absolute right to object to processing their data for direct marketing purposes, including profiling relevant to direct marketing.

Right of portability – in certain circumstances, Data Subjects have the right to move, copy or transfer his or her data to another data controller. This right is only relevant if the data is being processed on the basis of consent or for the performance of a contract and the processing is carried out by automated means. This right is different from the right of access and the types of information the Data Subject can get under the two separate rights may be different.

9.1 Right to Access Personal Data

9.1.1 Data Subjects have the right to access the personal information that is processed about them. This right is commonly referred to as subject access. Some types of Personal Data are exempt from the right of subject access and so cannot be obtained by making a Data Subject Access Request (DSAR). If there is any doubt in the types of data that can be supplied under a DSAR, the matter should be referred to the Executive Director for clarity.

9.1.2 Under the right to access to personal data the Data Subjects is entitled to:

(i) Be informed by any Data Controller whether Personal Data which relates to the individual is being processed by or on behalf of that Data Controller.
(ii) Be given a description of the information constituting Personal Data of which the individual is the Data Subject. Be given a description of the purposes for which their Personal Data is being or is to be processed.
(iii) Be given a description of the recipients or classes of recipients to whom their Personal Data is being or may be disclosed.

(iv) Be provided a copy of the information constituting any Personal Data of which the individual is the Data Subject in a form that is capable of being understood.

(v) Be provided details of any information available to the Data Controller as to the source of the Personal Data (where available) in a form that is capable of being understood.

(vi) Be provided (if specifically requested by the Data Subject) with the logic involved where the processing by automatic means of Personal Data of the Data Subject for the purpose of evaluating matters relating to the Data Subject e.g. performance at work, creditworthiness, has constituted or is likely to constitute the sole basis for any decision significantly affecting the Data Subject

9.1.3 Making a data access request:

(i) A Data Subject must make a Data Subject Access Request in writing to the Executive Director, a request sent by email or fax is acceptable. There is no charge to provide the Personal Data requested.

(ii) If there is uncertainty as to the identity of a Data Subject making the Data Subject Access Request, additional information should be requested from the Data Subject to verify their identity. This should be an official document - e.g. a drivers licence or passport.

(iii) A Data Subject is entitled to make a Data Subject Access Request via a Third Party. In this case the Executive Director needs to be satisfied that the Third Party making the request is entitled to act on behalf of the Data Subject. If the CRFM Secretariat believes an individual may not understand what information would be disclosed to a Third Party who has made a Data Subject Access Request on their behalf, the CRFM Secretariat may send the response directly to the individual (Data Subject) rather than the Third Party. The individual will then have the chance to review the data before deciding whether to share it with the Third Party.

(iv) In some cases, an individual will not have the mental capacity to manage their own affairs. However, it is reasonable to assume that an attorney with the authority to manage the individual's affairs will have the appropriate authority. Any concerns should be raised with the Executive Director.

(v) Further clarity regarding the information requested in the DSAR can be requested from the Data Subject. For example, if a Data Subject has requested Personal Data contained in emails, the CRFM Secretariat may ask for the dates the emails were sent.

(vi) If the response to a Data Subject Access Request involves providing information that relates to the Data Subject and another individual who can be identified from that information, either the consent of the individual is required, or it must be reasonable in all circumstances to comply with the request without the individual's consent. Any concerns should be raised with the Executive Director.

9.1.4 Responding to a Data Subject Access Request

(i) A Data Subject Access Request must be responded to no later than 30 days after it has been received by the Data Controller.

(ii) The 30-day period does not start until: The CRFM Secretariat as the Data Controller is satisfied as to the identity of the Data Subject making the request; and the additional information reasonably needed to find the Personal Data has been supplied by the Data Subject.

(iii) However, it is not acceptable to delay responding to a Data Subject Access Request unless more information is reasonably required to locate the Personal Data in question. The Data Subject has a right to see the information contained in the Personal Data rather than a right to see the documents that include that information.

(iv) The information requested must be provided in a permanent format - such as a computer printout, letter or form - unless: (a) the Data Subject agrees otherwise: (b) it is not possible to supply such a copy: or (c) it will involve undue effort; this includes very significant cost or effort to produce the information in hard copy. If this is the case, the CRFM Secretariat must still provide access to the information in another way. The CRFM Secretariat must also ensure that the information can be understood, for example, if there are any codes used, the CRFM Secretariat should explain what they mean.

9.2 Right to prevent processing likely to cause damage or distress

(i) A Data Subject has a right to object to processing only if it causes unwarranted and substantial damage or distress. If it does, they have the right to require an organisation to stop (or not to begin) the processing in question. In such circumstances the Data Subject may be able to require a Data Controller to not begin or to stop processing their personal Data. This right is limited to certain circumstances; if such circumstances do not apply the Data Controller has to provide an explanation to the Data Subject as to why it has no requirement to comply with the objection to processing.

(ii) There are a number of points to consider when deciding whether and to what extent there is an intention to comply with an objection to processing, such as, is the objection to processing in writing. An objection has to be in writing (which includes an email or fax). Once received, there is a time limit of 30 calendar days in which to provide a response to the Data Subject. The response must state what is intended to be done or if there is no intention to comply with the objection to processing and an explanation of why there is no requirement for the Data Controller to comply with the objection to processing.

(iii) Does the objection explain how the processing is / will cause unwarranted and substantial damage or distress? If it is not clear in the objection as to the extent of the problem the processing would be/is causing, the Data Subject may need to provide further clarification in order for a decision as to whether to comply with the objection to processing to be made or whether there is no requirement on the Data Controller to do so. A response (as set out above) must be provided to the Data Subject.

9.2.1 Processing that can be relied on to Legitimise the Processing

(i) The Data Subject has given their consent to the processing.

(ii) The processing is necessary for the performance of a contract to which the Data Subject is a party or for the taking of steps at the request of the Data Subject with a view to entering into a contract.
(iii) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
(iv) The processing is necessary in order to protect the vital interests of the Data Subject.

9.2.2 All objections to data processing are dealt with by the Executive Director. Any employee who receives an objection from a Data Subject must pass it to the Executive Director immediately.

9.3 The Right to Prevent Direct Marketing

9.3.1 Data Subjects have the right to prevent their personal Data being processed for direct marketing.

9.3.2 A Data Subject can at any time give written notice to the CRFM Secretariat as the Data Controller to stop (or not begin) using their Personal Data for direct marketing. Any Data Subject can exercise this right, and if such a notice is received it must be complied with in a reasonable period.

9.3.3 Data Subjects have the right to opt out of receiving marketing at any time. The CRFM Secretariat should not send marketing texts or emails to a Data Subject who has said they do not wish to receive them.

9.4 Rights to Correcting Inaccurate Personal Data

9.4.1 Where personal data is inaccurate, the Data Subject concerned has a right to rectify, block, erase or destroy the inaccurate information.

9.4.2 If an employee receives a request from a Data Subject to rectify, block, erase or destroy the inaccurate information the employee must pass this to the DPO or Executive Director immediately.

10.0 TRANSFER OF DATA TO UNAFFILIATED THIRD PARTIES

10.1 Any disclosure of personal data to third parties must be made in accordance with the applicable legal and contractual requirements and in accordance with the data protection / privacy preferences of the Data Subject.

10.2 This also applies to transfers within the CRFM as an institution. A request must be made to the Executive Director who will advise what requirements will be needed for approval.

11.0 SUPPLIER DUE DILIGENCE PROCEDURES

11.1 Due diligence procedures should be carried out during all supplier negotiations and on an ongoing basis.

11.2 Roles and responsibilities for supplier data protection compliance should be clearly articulated, in order to protect Personal Data, which is the responsibility of The CRFM Secretariat, maintain compliance with this Policy and any applicable legal requirements, and minimise operational and reputational risk.

12.0 DATA PROTECTION EVENT

12.1 All Employees should be vigilant of any Data Protection Event where Personal Data has been or is at risk of exposure to an unauthorised Third Party. Employees must immediately report such events to the Executive Director or their supervisor.

12.2 Below are four examples of situations where a Data Protection Event has occurred, although other situations are possible. These types of events can be deliberate or unintentional.

(i) Unauthorised Access to Personal Systems Containing Personal Data

An Employee, contractor, or third party accesses a system or data they should not have access to. This unauthorised access to Personal Data can occur with either electronic (e.g. email, database, etc.) or physical information (e.g. printed materials).

(ii) Loss or Theft of Data, Media and / or Devices

Electronic (e.g., cloud storage, backup tapes, CDs / DVDs, external drives, usb drives, laptop, mobile phone etc.) or physical information (e.g. printed materials) information is either lost or stolen by an individual or company. The information loss may occur due to the loss or theft of electronic files or physical media or devices (e.g. servers, desktops, laptops, hard disks, PDAs, mobile phones, external drives, etc.).

(iii) Inappropriate Disposal of Media and / or Devices

Physical or electronic files, media or devices are either not disposed when they are required to be or are insecurely disposed (for example, throwing sensitive documents in a standard rubbish bin) resulting in the exposure or potential exposure of Personal Data.

(iv) Improper and / or Unauthorised Communications

A mistake, incorrect process or unauthorised disclosure that results in Personal Data being communicated to an incorrect individual(s) or company (e.g., Wrong letter or email sent, incorrect name or address used, disclosure of other client account details etc.), or employee forwarding information or work emails containing another data subject's personal data to their personal email address.