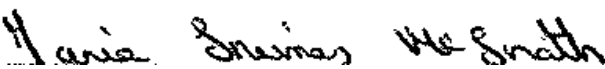





## Data Protection Policy and Procedures

<b>Revision:</b> A	<b>Department:</b> Governance, Strategy and Planning	<b>No:</b> DOCS 085
<b>Prepared by:</b>	 _____ Ms. Marie Grimes McGrath Data Protection Officer (DPO)	<b>Date:</b>  16/7/2020
<b>Approved by:</b>	 _____ Ms. Natalya Jackson Chief Executive Officer (CEO)	<b>Date:</b> 16/7/2020

**Review History**

<b>No.</b>	<b>Old revision status</b>	<b>New Revision Status</b>	<b>Comment</b>	<b>Date</b>	<b>Prepared By</b>	<b>Approved by</b>
1		A	Initial Issue	1/7/20	Marie Grimes McGrath	Natalya Jackson

## **CONTENT OVERVIEW**

	<b>Page No:</b>
1. Policy Statement	6
2. Purpose	6
3. Scope	6
4. Data Protection Legislation	7
5. Roles and Responsibilities	15
6. Subject Access Request Procedures	18
<i>Subject Access Request Procedures</i>	19
7. Data Breach Management Procedure	30
<i>Data Breach Management Procedure</i>	31
8. Organisational & Technical Measures for Security	40
9. Data Protection Impact Assessment	44
<i>Data Protection Impact Assessment Template</i>	45
10. Audits and Monitoring	70
11. References	71
12. Review	71
Appendix 1.1      Joint Data Controller Agreement Template	72
Appendix 1.2      Data Processor Agreement	81

## **DOCS 085 Data Protection Policy**

<b>CONTENTS</b>	<b>Page No:</b>
1.0 Policy Statement	6
2.0 Purpose	6
3.0 Scope	6
4.0 Data Protection Legislation	7
4.1 General Data Protection Regulation (GDPR)	7
4.1.1. Personal Data	8
4.1.2. Information protected under GDPR	8
4.2 Definitions	8
4.3 The General Data Protection Principles	10
4.3.1 Fair, Transparent and Lawful Processing	10
4.3.2 Purpose Limitation	11
4.3.3 Data Minimisation	11
4.3.4 Data Quality and Accuracy	11
4.3.5 Storage Limitation	11
4.3.6 Security and Confidentiality	12
4.3.7 Accountability and Fines	12
4.4 Data Subject Rights under GDPR	12
4.4.1 The right to be informed	12
4.4.2 The right of access to one's personal data	13
4.4.3 The right to Erasure (to be forgotten)	13
4.4.4 The right to Restrict Processing	14
4.4.5 The right to Correct Inaccurate or Incomplete Data	14
4.4.6 The right to Data Portability	14
4.4.7 The right to Object to Automated Decision Making	15
4.4.8 30-days Response Time applies to all Data Subject Rights	15
5.0 Roles and responsibilities:	15
5.1 Chief Executive Officer	15
5.2 Director of Governance, Strategy and Planning	15
5.3 Data Protection Officer	15
5.4 Service Managers/Heads of Departments / All Employees	17
5.5 IT Administrator	18
6.0 Subject Access Request Procedure	18
7.0 Data Breach Management Procedure	30
8.0 Organisational & Technical Measures for Security	40
8.1 Accountability & Compliance	40
8.2 Privacy by Design	40
8.3 Pseudonymisation	40
8.4 Encryption	41
8.5 Restriction	41
8.6 Third-Party Processors	41
8.7 Data Retention & Disposal	43

*Respect Service Collaboration Excellence Justice Creativity*

## CONTENTS

	Page No:
9.0 Data Protection Impact Assessments (DPIA)	44
10.0 Audits & Monitoring	70
10.1 Internal Compliance Audit	70
10.2 External Compliance Audit	70
10.3 Penalties	70
11.0 References	71
12.0 Review	71
13.0 Appendices	71
<b>Appendices:</b>	
Appendix 1.1 Joint Data Controller Agreement Template	72
Appendix 1.2 Data Processor Agreement Template	81
Appendix 2 Article 28 GDPR Requirement	92
Appendix 3 Data Protection ‘It’s Everyone’s Responsibility’	93
Appendix 4. Network Account Request Form	97
Appendix 4.1 How to Encrypt a Document	99
Appendix 4.2 Password Guidance for picking strong passwords	102
Appendix 5 Easy to Read Privacy Statement for a Data Breach	103

## **1.0 POLICY STATEMENT:**

Avista collects personal and sensitive information to effectively carry out its everyday business functions and activities for the individuals that it supports. In the course of the organisation's work, it is also required to collect and use certain information on current, past and prospective employee, volunteers, families, advocates, suppliers and others, with whom employees communicate with regard to continuity of service delivery. In all of the work Avista undertakes, the spirit of its Core Values enables the organisation to comply with, and commit to operating within all required legislation in a fair and transparent manner. Inherent in this policy is the dignity, respect and privacy that the organisation affords to those who avail of services, employees and third parties with regard to the integrity and security of their personal information.

The Data Protection Policy sets out how Avista seeks to protect personal and sensitive data and ensure that its employees, joint controllers and third party data processors understand the rules and regulations governing their use of data to which they have access during the course of their work and contact with AVISTA. Avista must comply with the Data Protection Principles set out in relevant Data Protection Law.

- Data Protection Acts 1988 and 2003 (parts not repealed).
- Data Protection Act 2018.
- ePrivacy Regulations 2011.
- General Data Protection Regulation (EU Regulation 679/2016).

Avista operates a *Privacy by Design* approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of its business.

## **2.0 PURPOSE:**

The purpose of this policy is to set out clearly to all staff and stakeholders how Avista must operate at all levels and roles across the organisation to ensure the organisation meets its legal, statutory and regulatory requirements under the Data Protection laws when processing all personal and sensitive information.

Avista has put comprehensive and effective governance structures, systems, policies and supporting procedures and guidelines in place to meet these provisions. These are outlined in this policy and supporting procedures. The aim of each of these measures is to ultimately minimise the risk of breaches and uphold the protection of personal and sensitive data in all activities Avista engages in.

## **3.0 SCOPE:**

This policy applies to all staff within Avista (*meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Avista in Ireland or overseas*).

This policy works with/alongside other AVISTA policies that all employees need to be aware of relating to data protection and include:

- AVISTA DOCS 050, Records Management Policy and Records Management Guidelines and Procedures.

*Respect Service Collaboration Excellence Justice Creativity*

- AVISTA DOCS 027, Policy on Administrative Access to Service User or Service-Related Records.
- AVISTA DOCS 028, Policy on Processing Freedom of Information Requests.
- AVISTA DOCS 014, Computer Network Policy.
- AVISTA Encryption Password Register Guidelines.
- AVISTA Encryption “How to Guide for Encrypting PDFs” Guidelines.
- AVISTA Legitimate Interest Policy.
- AVISTA DOCS 085, Data/Joint Data Controller and Third-Party Processor Agreement Templates (Appendices to this Policy).

#### **4.0 DATA PROTECTION LEGISLATION:**

The General Data Protection Regulation (GDPR) became effective on 25 May 2018.

#### **4.1 General Data Protection Regulation (GDPR):**

The *General Data Protection Regulation (GDPR) (EU) 2016/679* was approved by the European Commission in April 2016, and will apply to all EU Member States from 25th May 2018. As a 'Regulation' rather than a 'Directive', its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As Avista processes personal and sensitive information regarding individuals (*data subjects*), it is obligated under the General Data Protection Regulation (GDPR) to have systems and practices to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

#### **The Office of the Data Protection Commissioner (DPC):**

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

- The Data Protection Acts 1988 and 2003 (pre-25 May 2018), now replaced with the Data Protection Act 2018.
- General Data Protection Regulation enacted 25 May 2018.
- The Privacy and Electronic Communication (EU Directive) Regulations 2011.

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

Under the data protection laws, the DPC, as Ireland’s Data Protection Authority (*also known as the Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in Ireland.

Avista is registered with the DPC and appears on the Data Protection Register as a Data Protection Controller of personal/sensitive information and has a designated Data Protection Officer in accordance with GDPR requirements.

*Respect Service Collaboration Excellence Justice Creativity*

**There are two types of data defined in the Data Protection Legislation, personal data and special categories of data (hereinafter referred to as sensitive data).**

**4.1.1 Personal Data – Information protected under the GDPR is known as “personal data” and is defined as:** *“Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”*

**4.1.2 Information Protected under GDPR known as “Special Categories of Personal Data” is defined as:** *“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited, plus information on criminal convictions or investigations.”* Special categories of Personal Data will be hereafter referred to a sensitive data in this policy.

Avista will ensure that there are stringent control measures in place to protect the privacy, security and access to this data in line with GDPR Regulations.

#### **4.2 Definitions:**

**There are a number of definitions laid down under the General Data Protection Regulation (GDPR) that will be referred to throughout the Data Protection Policy to include:**

- **“Biometric data”** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- **“Pseudonymisation”** is a security measure whereby Avista can protect the identity of the person when recording or documenting their personal data by omitting or replacing information from their records. However, the text of the record will allow person/s to identify the data subject. For example, a summary document on a data subject maybe distributed prior to an MDT meeting where the name is omitted, but the data provided is so specific and unique that it allows the participants to identify the data subject.
- **“Consent”** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **“Cross Border Processing”** means processing of personal data which:
  - takes place in more than one Member State; or
  - substantially affects, or is likely to affect data subjects in more than one

*Respect Service Collaboration Excellence Justice Creativity*

Member State.

- **“Data controller”** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. **Avista is a Data Controller.**
- **“Data processor”** means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller. Avista may also be a data processor in situations where it has been contracted by another body, for example, the HSE to process data.
- **“Data protection laws”** means for the purposes of this document, the collective description of the GDPR and any other relevant data protection laws that the organisation complies with.
- **“Data subject”** means an individual who is the subject of personal data. Data Protection applies to the living person only.
- **“GDPR”** means the *General Data Protection Regulation (EU) (2016/679)*.
- **“Genetic data”** means personal data relating to the inherited or acquired genetic characteristics of a natural person, which gives unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- **“Processing”** means any operation or set of operations, which is performed on personal data, or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Profiling”** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **“Recipient”** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities, which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of this data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- **“Supervisory Authority”** means an independent public authority, which is established by a Member State, that being the “Data Protection Commissioner/ DPC in Ireland”.
- **“Third Party”** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority.
- **“Anonymisation”** This a process of either encrypting or removing personal identifiable information from a record, so that the persons to whom the data describes remains permanently anonymous.  
For example, redaction of a third-party personal information that is not related to a request for information.

*Respect Service Collaboration Excellence Justice Creativity*

### 4.3 The General Data Protection Principles:

There are seven GDPR Principles which Avista commits to uphold when processing data to include:

#### 4.3.1 Fair, Transparent and Lawful Processing:

The data is processed lawfully, fairly and in a transparent manner in relation to the data subject. Please refer to Avista Privacy Statement and Easy to Read Version available on [www.docservice.ie](http://www.docservice.ie), which will explain to data subjects why and how their data is being processed.

**In relation to personal data, the processing is lawful if at least one of the following applies:**

1. Processing is necessary for the **purpose of the legitimate interests** pursued by Avista or by the third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.
2. Processing is necessary for the **performance of a contract** to which the data subject is a party, or in order to take steps at the request prior to entering into a contact.
3. Processing is necessary for **compliance with a legal obligation** to which Avista is subject.
4. The data subject has **given consent** to the processing of his/her personal/sensitive data for one or more specific purposes.
5. Processing is necessary in order **to protect the vital interests** of the data subject or of another natural person.
6. Processing is necessary for the performance of a task carried out in **the public interest**.

Where Avista is unable to satisfy at least one of the above criteria for processing of personal data, it **does not have** a Fair, Transparent and Lawful Process to hold such data. (Article 6 of GDPR).

**In relation to sensitive data, the processing is lawful if at least one of the following applies:**

1. **Explicit consent:** The data subject has given their clear and unambiguous consent.
2. **Legal obligation** in relation to employment: The processing is necessary for the purpose of carrying out a legal obligation in relation to the field of employment.
3. **Vital interests:** The processing is necessary to protect the vital interests of the data subject, or of another person where the data subject is physically or legally incapable of giving consent.
4. **Legal claims:** The processing is necessary for the establishment, exercise or defense or legal claims, or whenever courts are acting in their judicial capacity.

*Respect Service Collaboration Excellence Justice Creativity*

5. **Healthcare:** The processing is necessary for the purposes of preventative or occupational medicines (i.e. healthcare purposes), for the assessment of the working capacity of the employee pursuant to their contract of employment, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems.
6. **Public Health:** The processing is necessary for reasons of public interest to ensure the necessary safeguards are in place.
7. **Archiving:** The process is necessary for reasons for archiving, scientific or historical research purposes, or for statistical reasons based on Regulatory Bodies and Legislation.
8. **Public Information:** The processing relates to data, which is manifestly made public to all data subjects or is in the public domain.

Where Avista is unable to satisfy at least one of the above criteria for processing sensitive data, it **does not have** a Fair, Transparent and Lawful Process to hold such data. (Article 9 of GDPR).

#### **4.3.2 Purpose Limitation:**

The data is collected for specified, explicit and legitimate purposes, and not further processed in the absence of consent from the data subject in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

#### **4.3.3 Data Minimisation:**

The data require is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. No unnecessary or additional data will be processed if the original purpose is satisfied.

#### **4.3.4 Data Quality and Accuracy:**

There is no tolerance for poor quality of data within Avista. It is important to ensure that the organisation considers the completeness, consistency and accuracy of the personal and sensitive data. Data should be factually accurate and a correct representation of reality (note, individuals can seek to view/acquire their data under a Subject Access Request, Section 6 of this Policy). Data held should be periodically checked for its accuracy and rectified as required.

#### **4.3.5 Storage Limitation:**

The data is kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was originally collected are processed. Please refer to DOCS 050, AVISTA Records Management Policy for the storage, retention schedule and confidential destruction of data.

#### **4.3.6 Security and Confidentiality:**

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

#### **4.3.7 Accountability and Fines:**

Requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles' ('accountability')*, and requires that Avista demonstrates how it complies with the principles, detailing and summarising the measures and controls that it has in place to protect personal information and mitigate the risks of processing. Fines can be imposed where there is evidence of non-compliance with the legislation, poor data management practice, data protection breaches, complaints to the DPC and non-compliance with this policy. A fine of 4% of annual budget can be applied. Avista is obliged under GDPR to retain a record of all personal/sensitive data collected, held and processed and will include:

- The name and details of the Controller, and where applicable, the Joint Controller, Third Party Processor.
- The purpose of processing.
- Categories of data subjects with whom data will be shared.
- Retention periods for each category of data.
- Transfer of data to other countries.
- Details of the technical and security measures in place for the data.

The Data Protection Officer will co-ordinate a database of all records, also known as a record of Data Processing Activities, and shall make it available for inspection by the Supervisory Authority at all times.

#### **4.4 Data Subject Rights Under GDPR:**

All persons have the right to have their personal/sensitive data processed in accordance with the Data Protection Acts.

##### **4.4.1 The right to be informed:**

Every data subject has right to be informed of the nature of the personal/sensitive data that is retained on them, the purpose for processing the data, and the access control measures in place, and the security and privacy of such data.

AVISTA has a link to its Privacy Notice on its website [www.docservice.ie](http://www.docservice.ie) and the organisation can provide a copy in physical and/or digital formats upon request. This notice provides the legal information on how the organisation handles, processes and discloses personal information.

The Privacy Notices will be updated by the Data Protection Officer in accordance with any changes to the GDPR Regulations and the Data Protection Act 2018.

#### **Employee Personal Data:**

*Respect Service Collaboration Excellence Justice Creativity*

As per the Data Protection Law guidelines, Avista does not use consent as a legal basis for obtaining or processing of data. As an employer, the organisation has a legitimate interest to process employee personal data for human resource purposes, among other activities, to maintain operational efficiency as an organisation.

All employees are provided with the organisation's Staff Handbook, which informs them of their rights under the data protection laws, and how to exercise these rights and are provided with a Privacy Notice specific to the personal information the organisation collects and process about them.

#### **4.4.2 The Right of Access to one's Personal Data:**

In the first instance, Avista encourages all data subjects to seek access to their personal data at local level through engagement with the relevant manager/designate, who will endeavour to process the request. In situations where this is not feasible, a formal request can be made.

This is called a Data Subject Access Request. Please refer to the **DOCS 085 Data Subject Access Request Procedure**, included in this Policy (Section 6).

Such information is provided free and is managed by the DPO and with prior verification as to the subject's identity (*i.e. verbally, electronic*).

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

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

#### **4.4.3 The right to Erasure (to be forgotten):**

Also, known as '*The Right to be Forgotten*', Avista complies with a data subject's right in this regard. Avista will ensure that personal data, which identifies a data subject is not kept longer than is necessary for the purposes for which the personal data is processed, where the processing is deemed unlawful or where consent has been withdrawn.

All personal/sensitive data obtained and processed by Avista is categorised in line with the value and status of the record, and is either given an erasure date, or is monitored so that it can be destroyed when no longer necessary. (Refer to Avista Data Retention Schedule in DOCS 050, Data Retention Schedule).

#### **4.4.4 The right to Restrict Processing:**

The data subject has the right to obtain from Avista the restriction of the processing of their personal/sensitive data where:

*Respect Service Collaboration Excellence Justice Creativity*

- Where an individual contests the accuracy of the personal data and the organisation is in the process of verifying the accuracy of the personal data and/or making corrections.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the organisation is considering whether it has legitimate grounds to override those of the individual.
- When processing is deemed to have been unlawful, but the data subject requests restriction as opposed to erasure.
- Where the organisation no longer needs the personal data, but the data subject requires the data to establish, exercise or defend a legal claim.

The Data Protection Officer reviews and authorises all restriction requests and actions, and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted, and the organisation has disclosed such data to a third-party, it will inform the third-party of the restriction in place, and the reason and re-inform them if any such restriction is lifted. The DPO will respond within a timely manner to the data subject.

#### **4.4.5 The Right to Correct Inaccurate or Incomplete Data:**

Under the GDPR, you have the right to request rectification of any inaccurate data held by Avista.

The Data Protection Officer will be notified of the data subject's access request to update personal data, and is responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, an addendum or supplementary statement will be recorded by the Data Protection Officer. Where notified of inaccurate data, the Data Protection Officer will rectify the error within 30 days in line with GDPR.

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

#### **4.4.6 The right to Data Portability**

Avista provides all personal information pertaining to the data subject to them on request and in a format that is easy to disclose and read. The organisation ensures that it complies with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this data will

not be transferred to protect the rights and freedoms of the other data subjects and third parties not related to the original request.

#### **4.4.7 The Right to Object to Automated Decision Making:**

Avista does not undertake automated decision-making or profiling of personal and sensitive data.

**4.4.8** 30-day response time by the Data Protection Officer applies to all subject rights. However, where it is deemed that a request may take longer to process, the Data Protection Officer will inform the Data Subject and a further two months can be applied to the processing of the request.

### **5.0 ROLES AND RESPONSIBILITIES:**

#### **5.1 Chief Executive Officer:**

The Chief Executive Officer (CEO) has overall responsibility for ensuring that Avista is upholding its legal responsibility to comply with the Data Protection legislation.

#### **5.2 Director of Governance, Strategy and Planning:**

The CEO has issued responsibility to the Director of Governance, Strategy and Planning as the designated role at executive level to lead out on the governance of data protection for Avista. Working with the Data Protection Officer, the Director of Governance, Strategy and Planning oversees the set up and operation of required data protection governance structures, systems, policy and practices that seek to ensure that Avista meets all requirements as set out in the GDPR Regulation.

#### **5.3 Data Protection Officer:**

The Data Protection Officer is the first point of contact for Avista with regard to all data protection issues. The Data Protection Officer is accountable to the Supervisory Authority (Data Protection Commissioner) on all matters.

The Data Protection Officer is responsible for:

- The Data Protection Officer, in consultation with The Executive, Senior Management and all stakeholders of Avista, will develop the processes and governance structures to meet the organisation's data protection obligations, and to ensure continued compliance with the legal and regulatory requirements of General Data Protection Regulations.
- Seeks to ensure that the rights of individuals with regards to the processing of personal information are fully upheld through data management practices across Avista. This will be undertaken through the development and implementation of the required data protection governance structures, systems with the supporting policies and procedures in place.
- Provides guidance and leads the implementation and roll out of these systems, seeking to ensure that all staff understand and implement such policies, procedures and guidelines.
- Supports business practice, functions and processes carried out by Avista, to ensure compliance with the data protection laws and its principles.
- Ensures that personal/sensitive data is only processed where the organisation has

*Respect Service Collaboration Excellence Justice Creativity*

verified and met the lawfulness of processing requirements.

- Ensures that the organisation only processes sensitive data in accordance with the GDPR requirements, having defined the lawful process/s to do so.
- Provide biannual reports to the CEO and Director of Governance, Strategy and Planning.
- Will ensure that systems and processes are in place to support consent at the time it is obtained, and can demonstrate evidence of such consent to the Supervisory Authority where requested.
- Seek to ensure that all employees are competent and knowledgeable about their GDPR obligations through provision of in-depth training in the data protection laws, principles, regulations and how they apply to their specific role and Avista.
- Will ensure that there are resources and supports in place for the service user through Easy to Read Documents that will assist and support them in their awareness and knowledge of their rights and freedoms under General Data Protection Regulations
- Have robust systems in place that seek to ensure individuals feel secure when providing the organisation with personal information and know that it will be handled in accordance with their rights under the data protection laws.
- Maintains a continuous programme of monitoring, review and compliance with the data protection laws, and to identify gaps and non-compliance before they become a risk, effecting mitigating actions where necessary to maintain compliance.
- Monitors the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements.
- Have robust and documented complaint handling and data breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.
- Have a dedicated audit and monitoring programme in place to perform regular checks and assessments on how the personal data the organisation processes is obtained, used, stored and shared. The audit programme is reviewed against the organisation's data protection policies, procedures and the relevant regulations to ensure continued compliance. Reports and outcomes with action plans will be provided to each manager/designate following an audit.
- Through support and audit of systems, seek to ensure that Data Retention Schedules are adhered to in accordance with Avista DOCS 050 Records Management Process, legal and statutory regulations. Ensure outcomes of audits are implemented in collaboration with the relevant manager/designate.
- Provide clear reporting lines and supervision with regards to data protection.
- Process all requests for information in relation to personal/sensitive data held or used about them, that will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- Co-ordinates training in data protection to ensure that employees, service users and stakeholders are aware of their own rights under the data protection laws, and are provided with information disclosures in the form of a Privacy Notice.
- Co-ordinate the development of a database of all the data processing activities across Avista in accordance with Article 30 requirements in consultation with the various areas. The organisation will have full oversight of the data risks

*Respect Service Collaboration Excellence Justice Creativity*

highlighted from the data processing activities, develop implementation plans to address, manage and mitigate such risks. The Data Protection Officer will make available to the Supervisory Authority Avista database of processing activities subject to request.

- Support Managers/Heads of Departments to complete Data Protection Impact Assessments (DPIAs) and will retain a database of DPIA's completed in order to monitor risks identified and support the implementation of proposed solutions and mitigating actions.
- The DPO will also review the DPIA's completed for the purpose of Research in Avista that have been approved by the Ethics Committee.
- Review and/or develop all Controller, Joint Controller and Third-Party Processor Agreements that are GDPR compliant in consultation with the relevant Department.
- Be available to support staff.

**The Data Protection Officer can be contacted at:**

**Address:** Marie Grimes McGrath  
Data Protection Officer  
Avista  
St Anne's Centre  
Sean Ross Abbey  
Roscrea  
Co. Tipperary  
E53 VK33

**Telephone:** 086 818 9201 / 0505 22046 Ext 297

**Email:** [mgrimesmcgrath@lim-docservice.ie](mailto:mgrimesmcgrath@lim-docservice.ie)

#### **5.4 Service Managers / Heads of Department/All Employees**

It is the responsibility of the local Service Manager and Heads of Departments to ensure that this policy is implemented in their areas of responsibility, and that all staff in their area of responsibility are made aware of their respective responsibility to safeguard all data in their area of work. They must ensure that all personal information held on computer or manually is accessed only on a "need to know" basis, and are informed of the procedure to manage an admin access request for information, which is detailed in the Policy on Administrative Access to Service User or Service Related Records, DOCS 027.

They must also ensure that staff members in their area of responsibility attend data protection training that is co-ordinated by the Data Protection Officer. They must actively engage with and seek support from the Data Protection Officer, as required.

## **5.5 IT Administrator:**

The IT Administrator is responsible for:

- Ensuring that all computers/laptops are compliant with the data protection legislation, and that the appropriate security measures are in place on all IT systems used to safeguard all personal data. For example, encryption of laptops, mobile phones, USB keys, use of passwords to access data.
- Ensuring that the disposal of old computers is in accordance with the Data Protection Act.

## **6.0 SUBJECT ACCESS REQUEST PROCEDURE:**

Subject Access Requests (SAR) are passed to the Data Protection Officer as soon as received, and a record of the request is noted. The type of personal data held about the individual is checked against the organisation's Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

**Please refer to Avista DOCS 085 Data Subject Access Request Procedure, as set out in this Policy. Section 6 for the guidelines on how an SAR can be made and what steps the organisation takes to ensure that access is provided under the data protection laws. The Data Protection Officer retains a log of all requests for information in the interest of accountability and fair and lawful processing of requests for information.**

**Avista**

**Data Protection Policy  
Subject Access Request Procedures**

<b>Revision:</b> <b>B</b>	<b>Department:</b> <b>Governance, Strategy and Planning</b>	<b>No:</b> <b>DOCS 085</b>
<b>Prepared by:</b>	<hr/> <b>Ms. Marie Grimes McGrath</b> <b>Data Protection Officer (DPO)</b>	<b>Date:</b>
<b>Approved by:</b>	<hr/> <b>Ms. Natalya Jackson</b> <b>Chief Executive Officer (CEO)</b>	<b>Date:</b>

### Review History

No.	Old Revision Status	New Revision Status	Comments	Date	Prepared by	Approved by
1		A	Initial Issue	8/7/2019	Marie Grimes McGrath	Natalya Jackson
2	A	B	Policy and Procedure update		Marie Grimes McGrath	Natalya Jackson

## **DOCS 085 – Subject Access Request (SAR) Procedures:**

<b>TABLE OF CONTENTS</b>	<b>Page</b>
1.0 Introduction:	22
1.1 The General Data Protection Regulation	22
2.0 What is Personal Information?	23
2.1. Personal Data	23
2.2. Information Protected	23
3.0 The Right of Access:	23
3.1 How to Make a Subject Access Request	24
3.2 Procedure for when a SAR is received	24
3.2.1. Identity Verification	24
3.2.2. Information Gathering	25
3.2.3. Information Provision	25
4.0 Fees and Timeframes:	25
5.0 Your Other Rights:	25
5.1 Automated Decision-Making	26
6.0 Exemptions and Refusals:	26
7.0 Submissions and Lodging a Complaint:	26
7.1 Supervisory Authority – Data Protection Commissioner	27
<b>Appendices:</b>	
Appendix 1	28

## 1.0 Introduction

This document supplements the Subject Access Request (SAR) provisions set out in Daughters of Charity Disability Support Services (hereinafter referred to as Avista), Data Protection Policy and Procedures, and provides the process for individuals to use when making an access request, along with the protocols followed by Avista when such a request is received.

Avista needs to collect personal information to effectively and compliantly carry out its everyday business functions and services and, in some circumstances, to comply with the requirements of the law and/or regulations.

As Avista processes personal information regarding individuals (*data subjects*), Avista is obligated under the General Data Protection Regulation (GDPR) and relevant data protection legislation to protect such information, and to obtain, use, process, store and destroy it, only in compliance with the GDPR and its principles.

## 1.1 The General Data Protection Regulation:

The General Data Protection Regulation (GDPR) gives individuals the right to know what information is held about them, to access this information, and to exercise other rights, including the rectification of inaccurate data. The GDPR is a standardised regulatory framework, which ensures that personal information is obtained, handled and disposed of properly.

As Avista is obligated under the GDPR and Irish Data Protection Laws, Avista must abide by the Regulations' principles, *which ensure that personal information shall be:*

- a) Processed lawfully, fairly, and in a transparent manner in relation to the data subject (*'lawfulness, fairness and transparency'*).
- b) Collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes (*'purpose limitation'*).
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed (*'data minimisation'*).
- d) Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is being processed, is erased or rectified without delay (*'accuracy'*).
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (*'storage limitation'*).
- f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical or organisational measures (*'integrity and confidentiality'*).

The Regulation also requires that 'the controller' shall be responsible for, and be able to demonstrate compliance with the GDPR principles' (*'accountability'*). Avista has

*Respect Service Collaboration Excellence Justice Creativity*

adequate and effective measures, controls and procedures in place, that protect and secure personal information and guarantee that it is only ever obtained, processed and disclosed in accordance with the relevant data protection laws and regulations.

## **2.0 What is Personal and Special Categories of Data?:**

Information protected under the GDPR are known as “personal data” and “Special Categories of Data (hereinafter referred to as sensitive data) also referred to as Sensitive Data”.

### **2.1 Personal Data – Information protected under the GDPR is known as “personal data” and is defined as:** *“Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”*

### **2.2 Information Protected under GDPR known as “Special Categories of Personal Data” is defined as:** *“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited, plus information on criminal convictions or investigations.”* Special categories of Personal Data will be hereafter referred to a sensitive data in this Procedure.

Avista will ensure that there are stringent control measures in place to protect the privacy, security and access to this data in line with GDPR Regulations.

Further information on what constitutes personal information and your rights under the data protection regulation and laws can be found at [www.dataprotection.ie](http://www.dataprotection.ie). You can also refer to Avista Privacy Statement on Avista website [www.docservice.ie](http://www.docservice.ie) on the ‘About Us’ page.

## **3.0 The Right of Access:**

Avista respects and is committed to the right of data subjects to access personal and sensitive information held regarding them. The Data Protection Officer is available to provide guidance and support to all parties to access their personal information through an informal pathway known as administrative access to records. This is a fair and transparent process to seek access to personal and sensitive data. However, under Article 15 of the GDPR, Avista ensures that it has a dedicated process in place, known as the Subject Access Procedure for providing access to personal information.

### **Where requested, Avista will provide the following information:**

- The purposes of the processing.
- The categories of personal data concerned.

*Respect Service Collaboration Excellence Justice Creativity*

- The recipient(s) or categories of recipient(s) to whom the personal data has been, or will be disclosed.
- If the data has been transferred to a third country or international organisation(s), *(and if applicable, the appropriate safeguards used)*.
- The envisaged period for which the personal data will be stored *(or the criteria used to determine that period)*.
- Where the personal data was not collected directly from the individual, any available information as to its source.

### **3.1 How to make a Subject Access Request (SAR):**

A subject access request (SAR) is a request for access to the personal information that Avista holds about you, which the Data Protection is required to provide under the GDPR *(unless an exemption applies)*. The information that is provided is covered in Section 3 of this document.

Through how the organisation does its work, it seeks that through transparent and open engagement the exchange of information between all shareholders, Avista seeks to enshrine an open spirit of sharing data held on individuals appropriately. In this regard, a data subject may discuss with their line manager access to information held by Avista on them. In the event that this is not feasible, the data subject will contact the Data Protection Officer to pursue their request for information.

You can make this request in writing using the details provided in Section 7, or you can submit your access request electronically. Where a request is received by electronic means, the Data Protection will provide the requested information in a commonly used electronic format *(unless otherwise requested by the data subject)*.

### **3.2 Procedure for when SAR is received:**

The Data Protection, in collaboration with the data subject, will take the following steps on receipt for a request for information.

#### **3.2.1 Identity Verification:**

Subject Access Requests (SAR) are passed to the Data Protection Officer as soon as received, and a record of the request is made. The SAR can also be sent directly to the Data Protection Officer at email address [mgrimesmcgrath@lim-docservice.ie](mailto:mgrimesmcgrath@lim-docservice.ie). The Data Protection Officer will use all reasonable measures to verify the identity of the individual making the access request, especially where the request is made using online services.

The Data Protection Officer will utilise the request for information to ensure that Avista can verify your identity, and where the Data Protection Officer is unable to do so, you may be contacted for further information, or you may be asked to provide evidence of your identity prior to processing any request. This is in order to protect your information and rights.

If a third party, relative or representative is requesting the information on your behalf, the Data Protection Officer will verify their authority to act for you and, again, may contact you to confirm their identity, evidence of your relationship to the data subject

*Respect Service Collaboration Excellence Justice Creativity*

and gain your authorisation prior to processing the any request.

### **3.2.2 Information Gathering:**

If you have provided enough information in your SAR to collate the information held about you, the Data Protection Officer will gather all documents relating to you and ensure that the information required is provided in an acceptable format. If the Data Protection Officer does not have enough information to locate your records, you will be contacted for further details. This will be done as soon as possible, and within the timeframes set out below.

### **3.2.3 Information Provision:**

Once the Data Protection Officer has collated all the personal information held about you, it will be sent to you in writing (*or in a commonly used electronic format if requested*). The information will be in a concise, transparent, intelligible and easily accessible format, using clear and plain language.

## **4.0 Fees and Timeframes:**

Avista aims to complete all access requests within 30 days of receipt of the request and verification and provide the information free of charge. Where the request is made by electronic means, AVISTA provides the information in a commonly used electronic format, unless an alternative format is requested.

Whilst Avista provides the information requested without a fee, further additional copies requested by the individual may incur a charge to cover administrative costs. This situation could arise where the request is considered to be voluminous incurring significant time to process the request. The Data Protection Officer will advise you of this decision and will offer you support to refine your request should you wish to do so.

Avista always aims to provide the requested information at the earliest convenience, but at a maximum and under regulation, 30 days from the date the request is received and verified. This 30-day timeline includes the weekend and public holidays. Therefore, it is imperative that when the Data Protection Officer issues a request for information to process a request that the relevant parties involved supply this information in a timely manner. However, where the retrieval or provision of information is particularly complex, or is subject to a valid delay, the period may be extended by a further two months. If this is the case, the Data Protection Officer will write to you within 30 days and keep you informed of the delay and provide the reasons.

## **5.0 Your Other Rights:**

Under the GDPR, you have the right to request rectification of any inaccurate data held by Avista. Where Avista is notified of inaccurate data, and agrees that the data is incorrect, Avista will amend the details immediately as directed by you, and make a note on the system (*or record*) of the change and reason(s).

Avista will rectify any errors within 30 days and inform you in writing of the correction and, where applicable, provide the details of any third-party to whom the data has been disclosed.

If, for any reason, Avista is unable to act in response to a request for rectification and/or data changes, a written explanation will be provided to you, and you will be informed of your right to complain to the Data Protection Commissioner, and to seek a judicial remedy.

In certain circumstances you may also have the right to request from Avista the erasure of personal data, or to restrict the processing of personal data, where it concerns your personal information, as well as the right to object to such processing. You can use the contact details for the Data Protection Officer in Section 7 to make such a request.

### **5.1 Automated Decision-Making:**

Avista does not undertake automated decision-making or profiling.

### **6.0 Exemptions and Refusals:**

The GDPR contains certain exemptions from the provision of personal information. If one or more of these exemptions applies to your subject access request, or where Avista does not act upon the request, you will be informed at the earliest convenience or, at the latest, within one month of receipt of the request.

Where possible Avista will provide you with the reasons for not acting, and any possibility of lodging a complaint with the Supervisory Authority and your right to seek a judicial remedy. Details of how to contact the Supervisory Authority can be found in Section 7 of this document.

### **7.0 Submission and Lodging a Complaint:**

To submit your Subject Access Request, you can contact the Data Protection Officer via email, or at the address below. You can also submit your request in writing using the *form in Appendix 1*, sending the request to:

#### **Dublin – North Tipperary/Offaly – Limerick:**

Marie Grimes McGrath  
Data Protection Officer  
Avista  
St. Anne's Centre  
Sean Ross Abbey  
Roscrea  
Co. Tipperary  
E53 VK33

**Telephone:** 086 818 9201 / 0505 22046 Ext 297

**Email:** [mgrimesmcgrath@lim-docservice.ie](mailto:mgrimesmcgrath@lim-docservice.ie)

If you are unsatisfied with Avista actions, or wish to make an internal complaint, you can contact Avista in writing at:

Marie Grimes McGrath

*Respect Service Collaboration Excellence Justice Creativity*

Data Protection Officer  
Avista  
St. Anne's Centre  
Sean Ross Abbey  
Roscrea  
Co. Tipperary  
E53 VK33

**Telephone:** 086 818 9201 / 0505 22046 Ext 297  
**Email:** [mgrimesmcgrath@lim-docservice.ie](mailto:mgrimesmcgrath@lim-docservice.ie)

### **7.1 Supervisory Authority:**

If you remain dissatisfied with Avista actions, you have the right to lodge a complaint with the Irish Data Protection Supervisory Authority. The Office of the Data Protection Commissioner can be contacted at:

Office of the Data Protection Commissioner  
Canal House  
Station Road  
Portarlinton  
R32 AP23  
Co. Laois

**Telephone:** 057 868 4800 / 076 110 4800  
**Lo Call Number:** 1 890 252 231  
**Fax:** 057 868 4757  
**E-mail:** [info@dataprotection.ie](mailto:info@dataprotection.ie)

## APPENDIX 1 SUBJECT ACCESS REQUEST FORM

Under the General Data Protection Regulation, you are entitled, as a data subject, to obtain from Avista confirmation as to whether Avista is processing personal data concerning you, as well as to request details about the purposes, categories and disclosure of such data.

You can use this form to request information, and access to any personal data Avista holds, about you. Details on where to return the completed form can be found at the end of the document.

### 1. Personal Details:

<b>Data Subject's Name:</b>		<b>DOB:</b>	___/___/___
<b>Home Telephone No:</b>		<b>Email:</b>	

**Data Subject's Address:**

**Are you currently supported by Avista?**

**Are you currently employed by Avista?**

**Are you a family member of someone currently supported by Avista?**

**Other –Please identify your relationship with Avista**

- Volunteer** ☐
- Supplier** ☐
- Retired Employee** ☐
- Agency Staff** ☐
- Consultant** ☐
- Contractor** ☐
- Student Placement** ☐
- Board Member** ☐
- Work Experience Placement** ☐

**Other please specify:** \_\_\_\_\_

**Any other information that may help us to locate your personal data – Please identify the location and, if possible, name the centre location:**

**Dublin** ☐ **Limerick** ☐ **Tipperary** ☐

**Service Name and Address:** \_\_\_\_\_

### 2. Specific Details of the Information Requested:

### 3. Representatives

*(only complete if you are acting as the representative for a data subject)*

*[Please Note: Avista may still need to contact the data subject where proof of authorisation or identity are required]*

<b>Representative's Name:</b>		<b>Relationship to Data Subject:</b>	
<b>Telephone No:</b>		<b>Email:</b>	

<b>Representative's Address:</b>
<b>I confirm that I am the authorised representative of the named data subject:</b> <b>Representative's Name:</b> _____ <b>Signature:</b> _____
<b>4. Confirmation</b>
<b>Data Subject's Name:</b> _____ [print name] <b>Signature:</b> _____ <b>Date:</b> ____ / ____ / ____
<b>5. Completed Forms</b>
<p><i>For postal requests please return this form to:</i>  Marie Grimes McGrath, Data Protection Officer, Avista, St. Anne's Centre, Sean Ross Abbey, Roscrea, Co Tipperary, E53 VK33.</p> <p><i>For email requests, please return this form to:</i> <a href="mailto:mgrimesmcgrath@lim-docservice.ie">mgrimesmcgrath@lim-docservice.ie</a></p>

## **7.0 DATA BREACH MANAGEMENT PROCEDURE**

**This Data Breach Management Procedure clearly SETS OUT what constitutes a Data Breach and the appropriate steps to take to contain the risk, reduce the impact on the Data Subject/s, Avista and to include notifications to the Supervisory Authority as is required. Please refer to Avista DOCS 085 Data Breach Management Procedure, as set out in this Section 7 of this Policy.**

All staff are responsible and accountable for reporting any data breach to his/her Line Manager and the Data Protection Officer, who will support and manage the data breach with the staff in the relevant area. It is important to remember that once the breach is identified, the clock starts to tick on the organisation's responsibility to report to the Data Commissioners Office within 72 hours of the breach being discovered.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of Avista and it is not about apportioning blame.

# AVISTA

## Data Protection Policy

### Data Breach Management Procedure

<b>Revision:</b> <b>B</b>	<b>Department:</b> <b>Governance, Planning and Strategy</b>	<b>No:</b> <b>DOCS 085</b>
<b>Prepared by:</b>	<hr/> <b>Ms. Marie Grimes McGrath</b> <b>Data Protection Officer (DPO)</b>	<b>Date:</b>
<b>Approved by:</b>	<hr/> <b>Ms. Natalya Jackson</b> <b>Chief Executive Officer (CEO)</b>	<b>Date:</b>

### Review History

<b>No.</b>	<b>Old Revision Status</b>	<b>New Revision Status</b>	<b>Comments</b>	<b>Date</b>	<b>Prepared by</b>	<b>Approved by</b>
1		A	Initial Issue	8/7/2019	Marie Grimes McGrath	Natalya Jackson
2	A	B	Policy and Procedure update		Marie Grimes McGrath	Natalya Jackson

*Respect Service Collaboration Excellence Justice Creativity*

## **DOCS 085 Data Breach Management Procedure**

<b>TABLE OF CONTENTS</b>	<b>Page</b>
1.0 Introduction/General/Data Protection Regulation (GDPR)	34
2.0 What is a Data Breach?	34
3.0 Roles and Responsibilities	34
3.1. The Data Protection Officer	34
3.2. All Staff	35
4.0 Procedure to be followed should a Data Breach occur	35
5.0 How to contact the Data Protection Officer	36
6.0 Audit	37
7.0 Review	37
<b>Appendices:</b>	
Appendix 1 – Data Protection Breach Incident Form	38
Appendix 2 - Flow Chart showing notification requirements	39

## **1.0 Introduction**

1.1 Avista is bound by the Irish Data Protection Act 2018, which was introduced on 25th May 2018, under the General Data Protection Regulations (GDPR) and the EU Electronic Communications Regulation 2011. The regulations place greater accountability and transparency obligation on Avista when processing personal and sensitive information. It also requires that Avista have stringent measures in place to ensure that the data is stored, managed and protected for the reason(s) that it was collected. Therefore, it is of paramount importance that all stakeholders are aware of, and implement Avista Data Protection Breach Management Procedure.

## **2.0 What is a Data Breach?**

2.1 A data breach is any unauthorised, unlawful or accidental disclosure, destruction, loss, alteration, use, recording, storing, distributing or access to personal data held by Avista. Examples of data breaches may include the following:

- a) Loss, theft or misplacement of IT equipment or devices containing personal data e.g. laptop, smartphone or USB key.
- b) Loss, theft or misplacement of a folder, briefcase or diary containing personal data.
- c) Human error resulting in an email or piece of post containing personal data being sent to the wrong person.
- d) An attack by a “hacker”, which results in unauthorised access to AVISTA computer systems.
- e) Unauthorised access to personal data as a result of a break-in.
- f) Unauthorised access to personal data by deception.
- g) Unauthorised access to personal data as a result of breaching access rights.
- h) Unforeseen circumstances such as flood or fire, where personal data is inaccessible.
- i) Where personal data has been deleted and the data cannot be restored.

This list is not exhaustive. If you have any concerns that a data breach may have occurred, please contact the Data Protection Officer.

## **3.0 Roles and Responsibilities:**

### **3.1 The Data Protection Officer:**

It is the responsibility of the Data Protection Officer to ensure that there is a robust Data Breach Management Procedure in place in Avista and that all staff are aware of and knowledgeable on the implementation of the procedure.

In the event that a data breach occurs, the data protection breach management procedure is evoked to support management and staff, and ensure the following actions are undertaken:

- Identification and classification of the data breach by reviewing the nature and sensitivity of the records breached.
- Containment and Recovery: Limit the scope and impact of the data breach on all parties.
- Risk assessment to identify immediate safeguards to minimise the potential adverse consequences from the data breach, and also to identify corrective measures.

*Respect Service Collaboration Excellence Justice Creativity*

- Notification of the data breach to the individuals involved if required, the Consumer Affairs Officer of the relevant HSE where the breach has occurred, and the Office of the Data Protection Commissioner.
- Evaluation and response to the data breach. The purpose of the evaluation/review is to ensure that the steps taken during the incident are appropriate, identify areas for improvement, and provide shared learning across Avista.

It is important that misuse or breaches of this procedure is reported to the Service Manager/designate and to the Data Protection Officer.

### **3.2 All staff:**

All Management and staff of Avista who create, receive and use personal information are responsible for the implementation of this procedure. All staff are responsible for respecting and protecting the privacy and confidentiality of the personal and sensitive information they process during the course of their work at all times.

### **4.0 Procedure to be followed should a Data Breach occur:**

4.1 It is vital that any suspected data protection breach be reported to the Data Protection Officer (DPO). Prompt reporting is crucial to ensure compliance with data protection law.

The Data Protection Officer will assist in determining whether in fact the incident is a breach and what action(s) and safeguards must be initiated.

4.2 A detailed account of the data breach should be recorded accurately on Avista Data Breach Incident Report Form, (Appendix 1), including the date and time the breach occurred; who reported the breach; description of the breach; details of any ICT systems involved, and a description of the nature of the data stored on the ICT system.

4.3 The Data Protection Officer will keep the CEO, ACEOs, Director of Governance, Strategy and Planning and relevant Manager/designated person informed of the data breach.

4.4 It is also the responsibility of the DPO to retain a log of all data breaches, which can be subject to inspection and audit by the Data Protection Commissioners Office.

**The DPO is required by law to report a data breach to the Irish Data Protection Commissioner within 72 hours of the breach occurring.**

Consideration is given to the severity of the breach, the nature and sensitivity of the data involved, the impact on the individual(s) whose data has been breached, and the reputational impact on Avista. This is communicated by means of a detailed written report of the data breach.

**In order for the Data Protection Officer to process the data breach, in compliance with data breach legislation, all data breaches need to be**

*Respect Service Collaboration Excellence Justice Creativity*

**communicated to the Data Protection Officer within 48 hours of the breach occurring.**

**The report will include the following:**

- The nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of personal data records concerned.
- A description of the likely consequence of the personal data breach.
- A description of the measures taken, or proposed to be taken by Avista to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Please refer to Appendix 1, Daughters of Charity Disability Support Data Protection Breach Incident Report Form that is to be submitted to the Data Protection Officer.

4.6 The Data Protection Officer is also required to inform the HSE Consumer Affairs Officer in writing, where the data breach has occurred. This will be a detailed written report of the data breach similar to that required by the Data Protection Commissioner.

4.7 The Data Protection Officer, in consultation with the CEO, will lead an investigation regarding all issues surrounding the data breach. The nature of such an investigation will vary from case to case, depending on the circumstances and seriousness of the data breach. The primary issue for consideration will be the question of informing those individuals directly affected by the loss, and how this might best be done. The Data Protection Officer will also take into consideration the recommendations from the Data Protection Commissioner and the Consumer Affairs Officer of the HSE.

4.8 Following the investigation, a thorough review of the incident will occur to ensure that steps taken during the management of the data breach were appropriate, areas of improvement for data processing and security were identified, and used for shared learning across Avista to enhance the transparency, accountability, safety and privacy of personal and sensitive information.

**5.0 How to contact the Data Protection Officer?**

It is the responsibility of the Data Protection Officer, under the Data Protection Act and Regulations to provide support, advice and guidance on the management of a data breach. Appendix 2 details the flow chart to be followed in the case of a data breach or suspected data breach. In line with best practice, all staff should contact the Data Protection Officer if they are unsure as to whether a data breach has occurred, for reassurance and support.

**Name:** Marie Grimes McGrath  
**Telephone:** 086 818 9201/0505 22046 Ext 297  
**Email:** [mgrimesmcgrath@lim-docservice.ie](mailto:mgrimesmcgrath@lim-docservice.ie)

**6.0 Audit:**

*Respect Service Collaboration Excellence Justice Creativity*

The Data Protection Officer will undertake audits on records in all areas on an annual basis, to ensure that Avista record management processes are compliant with legislation and regulations.

## **7.0**

### **Review:**

This procedure will be reviewed every three years or sooner if new legislation, codes of practice or national standards are introduced.

## **APPENDIX 1**

### **AVISTA**

#### **Data Protection Breach Incident Report Form**

<b><u>INCIDENT DETAILS</u></b>	
Area Name	
Description of the incident	
<u>Date and time incident occurred</u>	
Name of individual reporting the incident	
Incident reported to line manager and Data Protection Officer	
<u>Type of data involved. Any data of a sensitive nature</u>	
Number of individuals affected by the breach	
<u>Cause of the incident</u>	
Contributory Factors	
Were affected individuals contacted?	
Was the data encrypted or anonymised?	
Details of any IT systems involved in the breach	
<u>Safety Control measures enacted</u>	

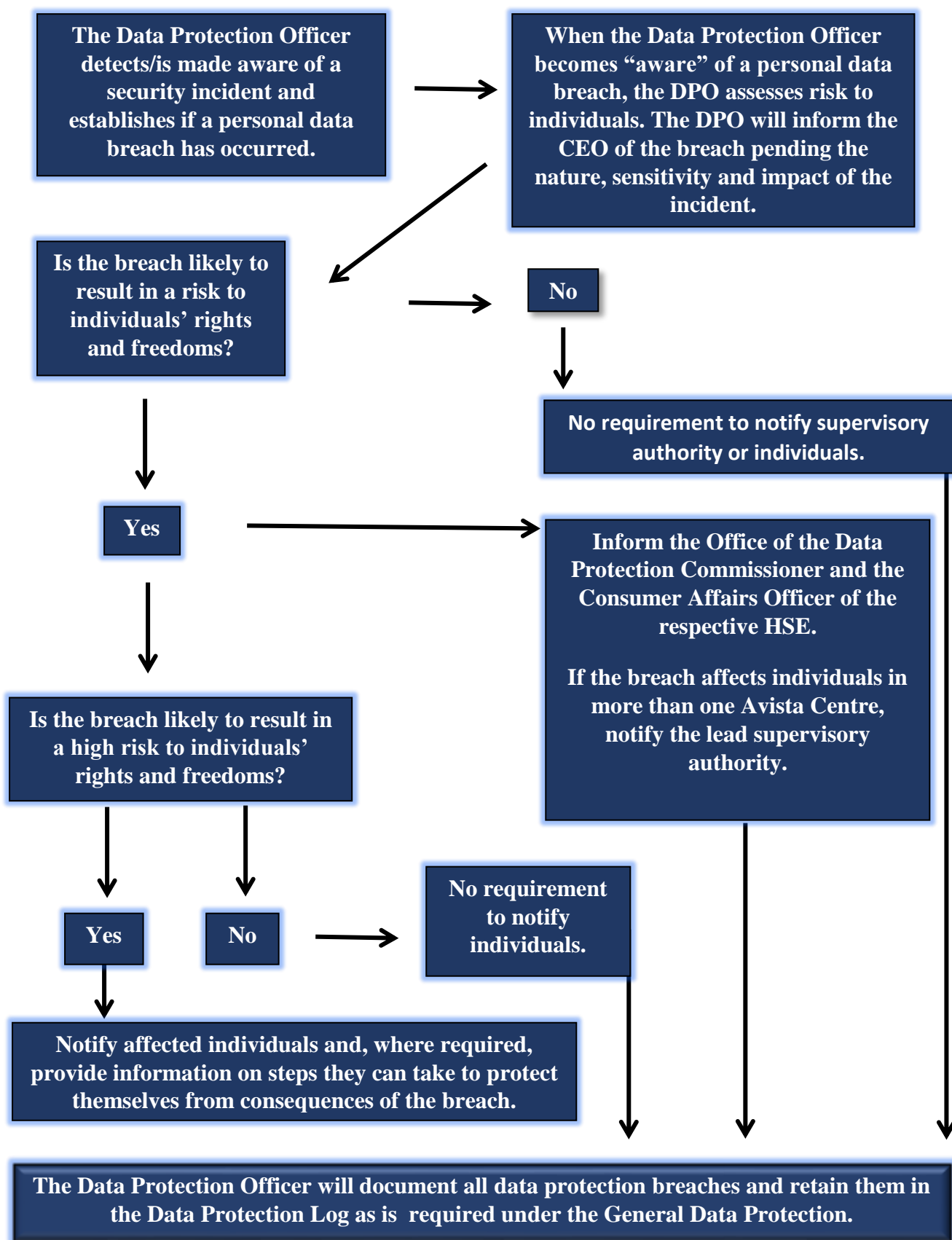
Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Received By DPO: \_\_\_\_\_ Date: \_\_\_\_\_

*Respect Service Collaboration Excellence Justice Creativity*

## **APPENDIX 2**

**Flow Chart showing notification requirements of a data breach to the Data Protection Officer:**



*Respect Service Collaboration Excellence Justice Creativity*

## 8.0 ORGANISATIONAL & TECHNICAL MEASURES FOR SECURITY AND SAFETY

### 8.1 Accountability and Compliance:

Due to the nature, scope, context and purposes of processing undertaken by Avista, the organisation carries out risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. The organisation is constantly endeavouring to implement adequate and appropriate technical and organisational measures, to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures throughout its documentation and practices.

### 8.2 Privacy by Design:

Avista operates a '*Privacy by Design*' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via its processes, systems and activities. The organisation has developed controls and measures (*detailed below*), that helps it enforce this ethos.

- Electronic collection (*i.e. forms, website, surveys etc.*) only have the fields that are relevant to the purpose of collection and subsequent processing. The organisation does not include '*optional*' fields, as optional denotes that it is not necessary to obtain.
- Physical collection (*i.e. face-to-face, telephone etc.*) is supported using scripts and internal forms, where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected.
- The organisation has bespoke agreements in place that are GDPR compliant with third-party controllers/processors who send personal information to the organisation (*either in the organisation's capacity as a controller or processor*). These state that only relevant and necessary data is to be provided as it relates to the processing activity the organisation is carrying out.
- The organisation has documented destruction detailed in DOCS 050 Records Management Policy procedures in place, where a data subject or third-party provides the organisation with personal information that is surplus to requirement.

### 8.3 Pseudonymisation:

The organisation utilises pseudonymisation, where possible, to record and store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (*personal identifiers*). Encryption and partitioning are also used to protect the personal identifiers, being kept separate from the pseudonymised data sets.

When using pseudonymisation, the organisation ensures that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation can mean that the data subject is still likely to be identified indirectly and as such, the organisation uses this technique in conjunction with other technical and operational measures of risk reduction and data protection. Avista is reducing the risk of a data breach by using pseudonymisation when documenting or transmitting personal sensitive data. This method of security can apply to multi-disciplinary team minutes, correspondences, third parties and emails. This is not an exhaustive list.

*Respect Service Collaboration Excellence Justice Creativity*

#### **8.4 Encryption:**

The organisation uses encryption as a further risk prevention measure for securing the personal data that it holds. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

The organisation password protects documents, and records the passwords in password registers. Please refer to Avista DOCS Policy 014 Information Technology, Email and Internet Policy. In particular, please refer to Network Account Request Form (Appendix 4.1 of this Policy), How to Encrypt a Document (Appendix 4.2 of this Policy), and Password Guidance for Picking Strong Passwords (Appendix 4.3 of this Policy).

#### **8.5 Restriction:**

The organisations *Privacy by Design* approach means that it uses service-wide restriction methods for all personal data activities. Restricting access is built into the foundation of Avista processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by Authorised staff.

#### **8.6 Third-Party Processors:**

Avista utilise external processors for certain processing activities (*where applicable*). The organisation uses information audits to identify, categorise and record all personal data that is processed outside of Avista, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing includes (but is not limited to):

- IT Systems and Services.
- Legal Services.
- External Auditors.
- Human Resources Systems.
- Payroll.
- Hosting or Email Servers.
- HIQA.
- NIMS.
- NIDD.
- HSEA.
- External Consultants/Pharmacies/General Practitioners/Training Consultants.

Avista endeavours to apply due diligence procedures and measures to review, assess and background check all processors prior to forming a business relationship. The organisation obtains, where required, company documents, certifications, references and ensures that the processor is adequate, appropriate and effective for the task the organisation is employing them for. Such security checks will be reflected in Avista Data Controller/Sharing/Processing Agreements. The Data Protection Officer will support all areas in the development of such agreements and retains a log of all agreements. Please refer to the Joint Data Controller Agreement Template (Appendix 1.1 of this Policy), and the Data Processor Agreement Template (Appendix 1.2 of this Policy).

The Data Protection Officer will monitor their processes and activities during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance.

The continued protection of data subjects' rights and the security of their personal information is always the organisation's top priority when choosing a processor and the organisation understands the importance of adequate and reliable outsourcing for processing activities, as well the organisation's continued obligations under the data protection laws for data processed and handled by a third-party.

***The organisation will have bespoke Service Level Agreements (SLAs) with the HSE and Regulatory Authorities, Contracts with each Processor as per the services provided, and an agreed Processor/Data Controller/Data Sharing Agreement in place with the relevant party. Please refer to Appendix 2, Article 28 GDPR requirements that sets out the mandatory requirements for all agreements. This is a standalone GDPR document under Data Protection Law:***

- The processor's data protection obligations.
- The organisation's expectations, rights and obligations.
- The processing duration, aims and objectives.
- The data subject's rights and safeguarding measures.
- The nature and purpose of the processing.
- The type of personal data and categories of data subjects.

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without the organisation's prior specific authorisation, and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

***The Processor Agreement and any associated contract reflects the fact that the processor:***

- Processes the personal data only on the organisation's documented instructions.
- Seeks the organisation's authorisation to transfer personal data to a third country or an international organisation (unless required to do so by a law to which the processor is subject).
- Shall inform the organisation of any such legal requirement to transfer data before processing.
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality, or are under an appropriate statutory obligation of confidentiality.
- Takes all measures to security the personal data at all times.
- Respects, supports and complies with the organisation's obligation to respond to requests for exercising the data subject's rights.
- Assists Avista in ensuring compliance with its obligations for data security, mitigating risks, breach notification and privacy impact assessments.

*Respect Service Collaboration Excellence Justice Creativity*

- When requested, deletes or returns all personal data to Avista after the end of the provision of services relating to processing, and deletes existing copies where possible.
- Makes available to Avista all information necessary to demonstrate compliance with the obligations set out in the agreement and contract.
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract.
- Informs Avista immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract.

## **8.7 Data Retention and Disposal:**

Avista has defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects (*e.g. shredding, disposal as confidential waste, secure electronic deletion*) and prioritises the protection of the personal data in all instances. Please refer to DOCS 050 AVISTA Records Management Policy to implement the organisation's data retention and disposal procedures.

## **9.0 DATA PROTECTION IMPACT ASSESSMENTS (DPIA):**

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by Avista. The organisation, therefore, utilises several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, the organisation utilises proportionate methods to map out and assess the impact ahead of time.

Where Avista must, or are considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, the organisation will carry out a Data Protection Impact Assessment (DPIA) *(sometimes referred to as a Privacy Impact Assessment)*. *It is the responsibility of the Data Protection Officer to ensure that such DPIAs are completed through the provision of advice, guidance and support to the relevant Departments. Records of Avista DPIAs are monitored and retained by the Data Protection Officer. This also extends to DPIAs that are required as part of a submission to Avista Ethics Committee.*

**Please refer to the DOCS 085 Data Protection Impact Assessment Procedure, as set out in this Section 9 of this Policy.**

# AVISTA

## Data Protection Impact Assessment Template

<b>Revision:</b>  <b>A</b>	<b>Department:</b>  <b>Governance, Strategy and Planning</b>	<b>No:</b>  <b>DOCS 085</b>
<b>Prepared by:</b>	<div><div>_____</div><div><b>Ms. Marie Grimes McGrath</b> <b>Data Protection Officer (DPO)</b></div><div>_____</div><div><b>Mr. Tom McArdle</b> <b>IT Administrator</b></div></div>	<b>Date:</b>
<b>Approved by:</b>	<div><div>_____</div><div><b>Ms. Natalya Jackson</b> <b>Chief Executive Officer (CEO)</b></div></div>	<b>Date:</b>

### Review History

No.	Old revision status	New Revision Status	Comment	Date	Prepared By	Approved by
1		A	Initial Issue	04/11/19	Marie Grimes McGrath, Tom McArdle	Natalya Jackson

## **DOCS 085 Data Protection Impact Assessment Template**

<b>TABLE OF CONTENTS</b>	<b>Page</b>
1.0 Introduction	48
2.0 Data Protection Impact Assessments (DPIA):	48
2.1 Assessment Requirements	49
2.2 Impact Assessment Team	49
3.0 DPIA Stages:	50
3.1 Identify the Need for a Data Protection Impact Assessment	51
3.2 Project Brief and Plan	53
3.3 Identify the Risks and Privacy Issues	59
3.4 Identify and Evaluate Privacy Solutions	62
3.5 Integrate Outcomes	64
4.0 Authorisation and Recording:	66
<b>Appendices:</b>	
Appendix 1: Types of Privacy Risk	67
Appendix 2: Guidance for Completing a Risk Register	68
Appendix 3: Checklist for a DPIA	69

## 1.0 Introduction:

The terms Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) are often used inter-changeably within the security and privacy worlds, but can sometimes have different meanings. The PIA is a long-standing term for an assessment that looks at the effects and risks of privacy of a project or process, with privacy being considered and not just the data protection implications. Whereas, DPIA is the term the GDPR utilises for the risk-based approach and pre-assessments for high-risk processing.

For the purposes of this document, Avista (*hereinafter referred to as the “AVISTA”*) expands upon the GDPR requirements as set out in the Regulation and encompasses data protection and privacy, with all aspects and facets being included and considered. The organisation uses the DPIA reference, but aims to exceed the Regulation requirements, using Article 29 Working Party '*Guidelines on Data Protection Impact Assessment (DPIA)*', as well as the UK Information Commissioner's reference to "*Privacy Impact Assessments*" (PIA).

## 2.0 Data Protection Impact Assessments (DPIA):

Data Protection Impact Assessments (DPIA) are a requirement of the GDPR and are a tool that can assist those with data protection obligations, in identifying the risks associated with data processing and posed to data subjects. It enables a pre-emptive approach to assess the risks and apply corrective actions and mitigating controls before a breach occurs.

This Data Protection Impact Assessment (DPIA) document accompanies the organisation's GDPR Policy and Procedures, and aids in the privacy by design ethos advocated in the ***General Data Protection Regulation (GDPR) (EU)2016/679***. Article 35 of the Regulation provides the situations and provisions for DPIAs, and require those obligated under the GDPR, to have processes in place to assess data protection risks, and identify when a DPIA is required.

The overall aim of the organisation's DPIA is to apply solutions and mitigating actions, where a processing activity is deemed likely to cause a high risk to one or more individuals. The mitigating actions are then implemented into the project plan, and then reassessed to ensure that the risk(s) has been eliminated or reduced to an acceptable level. ***The overall scope of the risk solutions is to either:***

- Eliminate.
- Reduce.
- Accept.

Where an impact assessment report indicates that the processing involved will, or is likely to result in a high risk to an individual(s), and the organisation is unable to mitigate such risk(s) with appropriate measures or controls, the organisation consults the Supervisory Authority prior to the processing taking place.

**Please note that Avista has a separate DPIA Document for the purpose of conducting of research that is unique and identifiable to Avista Ethics Committee.**

## 2.1 **Assessment requirements:**

Individuals have an expectation that their privacy and confidentiality will be upheld and respected, whilst their data is being stored and processed by any organisation. When the risks of processing are high, the organisation employs the use of impact assessments to assess the risk, the impact and the likelihood, and to document the origin, nature, accuracy, and severity of that risk, along with the processing purpose, reasons and mitigating measures and/or proposed solutions.

The organisation relies on Article 35(3) conditions and accompanying Recitals as to when completing an impact assessment is necessary. This list is included below. However, it is not exhaustive, and the organisation assesses each process activity on its own merits and carries out a DPIA, where the organisation believes that the processing is likely to result in high risk.

***Pursuant to Article 35(3) and Recitals 84, 89-96, the organisation considers processing that is likely to result in a high risk to include: -***

- Systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person, or similarly significantly affect the natural person(s).
- Processing on a large scale of special categories of data.
- Processing on a large scale of personal data relating to criminal convictions and offences.
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV).
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual.
- Those involving the use of new technologies.
- New processing activities not previously used.
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects.
- Processing activities making it difficult for the data subject(s) to exercise their rights.

## 2.2 **Impact Assessment Team:**

A lead is appointed to carry out the DPIA, follow the process, record the necessary information and report the results to the Senior Management Team. All DPIAs are carried out in conjunction with the Data Protection Officer, who provides advice and support for the compliance of the processes with the GDPR rules. Where there are systems, and/or new technologies involved, the DPIA team also includes an IT representative.

If the screening questions indicate that an impact assessment is required, the DPIA Team Lead, in conjunction with the Data Protection Officer, will assess the processing operations that will be involved in the DPIA (*using the positively answered screening questions*) and decide if any further team members are required.

***This includes choosing specific team members who:***

- Understand the project's aims and the organisation's objectives.
- Authority to influence the design and development of the project and participate in decisions.
- Expertise in data protection and compliance matters.
- Ability to assess and suggest solutions to risks and develop mitigating actions.
- Ability to communicate effectively with stakeholders and management.
- The DPIA Team Lead can at any point in the PIA process, engage other members to assist in specific areas as they deem fit or necessary.
- The Data Protection Officer will retain a record of all DPIAs completed across the organisation.

### **3.0 DPIA Stages (see Appendix 3 for checklist):**

The DPIA procedure has been divided into the following stages to ensure that all aspects are covered, reviewed and documented. Each stage is covered in detail under its category heading.

**Stage 1:** *Identify the Need for a Data Protection Impact Assessment* - review the GDPR Article 35(3) conditions and use the screening questions to ascertain if the processing is likely to result in high risk to individuals.

**Stage 2:** *Project Brief and Plan* - description of the information flows, what data is being processed, where it is coming from, who it is going to etc.

**Stage 3:** *Identify the Risks* - risks will include those to individuals, the organisation and compliance (law/regulation breaches) and after speaking to management, employees and stakeholders.

**Stage 4:** *Identify and Evaluate Privacy Solutions* - develop and document corrective actions, solutions and mitigating controls that can reduce or eliminate the risks. Evaluate costs and benefits of each solution.

**Stage 5:** *Integrate Outcomes* - the solutions and actions to reduce/remove the risks must be added back into the project plan, so that the risks can be reassessed with the mitigating actions in place. The Data Protection Officer will monitor the risks and solutions identified from the DPIA, and will support the relevant team for the duration of the project.

**Stage 6:** *Authorisation and Recording* - all stages of the DPIA must be recorded, using the provided templates, and sign off must be obtained from the DPIA Lead, Data Protection Officer and Director/Senior Manager.

**The Data Protection Officer will record and retain a copy of all DPIAs completed across the organisation.**

### 3.1 Identify the Need for a Data Protection Impact Assessment:

Not all processing activities will require a DPIA to be completed. It is, therefore, essential that the organisation carries out a check and uses its predefined screening questions to ascertain which, if any, of the high-risk operations the organisation intends to carry out, will require an impact assessment to be completed.

The questions provided in the screening template cover most of the risks that could be classed as high to a data subject, and can be used prior to each assessment proposal. However, the organisation also judges each processing operation on its own merits and add questions if they are specific to the project or objective.

The organisation also starts its internal and external consultations at this stage and involves stakeholders, employees, senior management and any associated third parties who play a part in the processing, or can lend insight and feedback to the processing operation and proposed risks. If any risks are identified via consultations, these are also added to the impact assessment template.

*The below screening questions apply to all business types and sectors. However, you are free to add/edit/remove any questions as application to your company.*

**Note:** Each screening question should be answered, and you should add any new relevant question at the bottom dependant on the risk and/or processing operation you are assessing. These screening questions will help you to identify if a DPIA is required and provide valuable insight into the processing operation risks and the areas to focus on.

REF	SCREENING QUESTION	YES	NO	N/A	NOTES
1	Does the processing require systematic and/or extensive evaluation ( <i>via automated means</i> ) of personal aspects of an individual(s)?				
2	Will decisions be based on such evaluations that are likely to produce legal effects concerning the individual(s)?				
3	Is the processing on a large scale and involves special categories of data?				
4	Is the processing on a large scale and involves data relating to criminal convictions and offences?				
5	Does the processing involve systematic monitoring of a publicly accessible area on a large scale? ( <i>i.e. CCTV</i> ).				
6	Will the project involve the collection of new information about individuals?				
7	Will the project compel individuals to provide information about themselves?				
8	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?				

*Respect Service Collaboration Excellence Justice Creativity*

**Note:** Each screening question should be answered, and you should add any new relevant question at the bottom dependant on the risk and/or processing operation you are assessing. These screening questions will help you to identify if a DPIA is required and provide valuable insight into the processing operation risks and the areas to focus on.

REF	SCREENING QUESTION	YES	NO	N/A	NOTES
9	Is the information about individuals likely to raise high risk privacy concerns or expectations?				
10	Will information about individuals be disclosed to organisations or people, who have not previously had routine access to the information or a third-party without adequate safeguards in place?				
11	Does the processing involve the use of new technology or systems, which might be perceived as being privacy intrusive?				
12	Could the processing result in decisions being made, or action being taking against individual(s), in ways that could have a significant impact on them?				
13	Will the project require you to contact individuals in ways which they may find intrusive?				
14	Will any of the processing activities make it difficult for the data subject(s) to exercise their rights?				
15	Will the operation involve processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects?				
16	Will the processing involve individuals who are considered 'vulnerable'?				
17	Does the processing operation involve any significant risk of the personal information being leaked or accessed externally?				

If you answered **NO** to all the screening questions, it is unlikely that you will need to carry out a DPIA. You should retain a copy of this completed sheet, along with your justification for any your answers in the notes section.

If you answered **YES** to one or more of the screening questions, you should proceed through the DPIA stages and complete the full assessment. When completed, a copy of your finished screening questions, answers and notes should be retained along with the recorded DPIA documents.

### 3.2 DPIA Plan and Brief:

Where data is obtained and how it is processed, stored and destroyed, is an essential part of a data protection impact assessment and as such, the organisation utilises its existing Information Audit data to complete this part of the assessment.

*Respect Service Collaboration Excellence Justice Creativity*

The information audit enables the organisation to identify, categorise and record all personal information obtained, processed and shared by the organisation in its capacity as a controller/processor and includes:

- What personal data the organisation holds.
- Where it came from.
- Who the organisation can share it with?
- Legal basis for processing it.
- What format(s) is it in.
- Who is responsible for it?
- Access level (*i.e. full, partial, restricted etc.*).

The organisation uses the data on the existing Information Audit to help it populate the below project brief and plan. This plan serves as the basis for carrying out the audit, and for demonstrating the organisation's compliance with the GDPR impact assessment requirements. The organisation understands that an incomplete understanding of how information is obtained, processed and stored, can be a risk itself and must be documented to ensure a full assessment is possible.

***Examples:***

- (a) If the organisation does not know how data has been obtained, it is unlikely to be able to verify the consent.
- (b) If the organisation has not documented and evidenced that it has met all the lawfulness of processing conditions when the data was obtained, the organisation may be unfairly processing information, or be preventing an individual from exercising their data protection rights.

How information audits are documented is bespoke to each organisation and can involve several methods to ensure a complete profile of the data is obtained and accessible. The organisation uses one or more of the below methods for recording the personal information obtained, processed, stored and transferred by it: -

- Information Audit.
- Data Processing Activities.
- Information Flow Charts.
- Information Asset Register.
- Risk Assessments.
- Service User Health Care Plans and Multidisciplinary Reports.
- Records collated relevant to function of the Department, e.g. Human Resource, Finance, Central Management Records.

**Note:** This is not an exhaustive list.

The project brief and plan templates also consist of the project background information, such as objectives, purpose, proposals, consultation reviews, outline/summary and previous DPIAs. This gives an overall picture of the project and enables a better assessment of the privacy impact and risks.

The third part of the project brief and plan template is the main assessment questions, which provides the basis for identifying the risks. The questions are predefined. However, the organisation does add to these if the project requires specific questions or assessment criteria.

A DPIA is intended to be flexible and can accommodate any form of processing assessment. The responses to the assessment questions then gives the organisation the issues and associated risks that are transferred over to the Privacy Issues and Risks template, detailing who is impacted, how they are impacted and providing a risk rating.

DPIA PROJECT BRIEF AND PLAN		
<b>PROJECT NAME:</b>		<b>DIRECTIONS:</b> <ol style="list-style-type: none"> <li>1. Complete each section and answer all the assessment questions.</li> <li>2. Use the reference number to refer to any responses that pose a risk and complete the Privacy Issues and Risks template.</li> <li>3. Provide as much detail as possible to ensure a complete assessment is made.</li> </ol>
<b>DPIA LEAD:</b>		
<b>DATE:</b>		
<b>CONTACT DETAILS:</b>		
1. PROJECT BACKGROUND		
1.1	<b>PROJECT SUMMARY:</b> Give an outline of the project, the processing and describe what is being planned.	
1.2	<b>OBJECTIVES:</b> - What are the aims of this project? What do you want to achieve from the processing? Why is it important/beneficial?	
1.3	<b>PURPOSE:</b> - What is the purpose of obtaining and processing the data?	
1.4	<b>POTENTIAL RISKS:</b> - Prior to carrying out the assessment question section, are there any privacy impacts or risks that have already been identified?	
1.5	<b>CONSULTATIONS:</b> - What insights or feedback have been obtained through consultations with stakeholders, third-parties and employees?	

*Respect Service Collaboration Excellence Justice Creativity*

1. PROJECT BACKGROUND		
1.6	<b>EXISTING DATA:</b> - Have any previous DPIAs or compliance assessments been carried out on similar processing activities that can provide guidance for this assessment?	
1.7	<b>SYSTEMS/TECHNOLOGY:</b> - If the processing involves the use of new technology or systems, provide any relevant information obtained from the initial implementation assessment of such systems.	
1.8	<b>OTHER:</b> - Detail any other information or suggestions that can add to the impact assessment?	
2. INFORMATION AUDIT		
PERSONAL DATA	JUSTIFICATION	PROCESSING ACTIVITY
What data will be collected?	Why does this data need to be collected? Is there anything you can omit if not necessary?	What processing operation(s) will the data be used for?
Name		
Address		
Postcode		
DOB		
Age		
Gender		
Email Address		

*Respect Service Collaboration Excellence Justice Creativity*

PERSONAL DATA		JUSTIFICATION	PROCESSING ACTIVITY
<i>What data will be collected?</i>		<i>Why does this data need to be collected? Is there anything you can omit if not necessary?</i>	<i>What processing operation(s) will the data be used for?</i>
Home Tel No.			
Mobile Tel No.			
PPS No.			
Medical Card No.			
Income/Expenses			
Employment Data			
Ethnic Origin			
Religion			
Health Details			
Convictions			
Credit Data			
Other			

### 3. ASSESSMENT QUESTIONS

REF	ASSESSMENT QUESTIONS	RESPONSE
3.1	<i>What is the legal basis for processing the information?</i>	
3.2	<i>Who will have access to the information?</i>	
3.3	<i>Will there be restrictions applied to access?</i>	
3.4	<i>Does the data need to be transferred to a third-party?</i>	
3.5	<i>Do you have safeguards in place for transferring?</i>	
3.6	<i>Will you need to obtain consent to process?</i>	
REF	ASSESSMENT QUESTIONS	RESPONSE
3.7	<i>How will consent be obtained and the right to withdraw consent be made available?</i>	
3.8	<i>Will you have control over the data and be able to update/complete it where applicable?</i>	
3.9	<i>Will you be using data minimisation techniques?</i>	
3.10	<i>Will data be encrypted and/or pseudonymised?</i>	

*Respect Service Collaboration Excellence Justice Creativity*

3.11	<i>How will information be destroyed after it is no longer necessary?</i>	
3.12	<i>How will information be stored?</i>	
3.13	<i>Will you be able to act on all rights of data subjects? (i.e. objections, rectifications, erasure, access etc)</i>	
3.14	<i>Will you be able to meet the deadline for supplying information?</i>	
3.15	<i>Does the processing operation require the Supervisory Authority to be notified?</i>	
3.16	<i>What security measures are in place to protect identifiable information?</i>	
3.17	<i>Have all employee, agents and third-parties involved in the project been trained on the data protection regulations and impact risks?</i>	
3.18	<i>What consultations are involved in identifying the privacy issues and risks associated with this project?</i>	
3.19	<i>Will personal data be transferred to a third country or international organisation outside the EU? If yes, what safeguards and Chapter V GDPR measures are in place?</i>	
3.20	<i>Detail any other factors or information that can assist in this Privacy Impact Assessment.</i>	

*Respect Service Collaboration Excellence Justice Creativity*

### 3.3 Identify the Risks and Privacy Issues:

Using the responses obtained from answering the assessment questions, the organisation is now able to identify the privacy issues and associated risks, and record who these risks will impact. Risks will usually fall into one of three categories: -

- **Risks to Individuals** - Any risk that affects a data subject, their data, their privacy, or their rights is classed as a risk to an individual. Inadequate disclosure controls, consent issues, processing purposes and surveillance methods are just a few of the issues that may result in risks to individuals.
- **Compliance Risks** - These can arise where the assessment response indicates that a breach of laws, legislation and/or regulations will occur if the processing goes ahead. This can include non-compliance with the GDPR, PECR, or human rights legislation.
- **Corporate Risks** - Risks that will affect the business, including reputation, revenue, fines and sanctions. These will mainly arise where the initial collection, consent, disclosures, sharing and storage of the personal information have not been complied with, or where record keeping is ineffective.

Once the risks have been identified, the below risk matrix is used to give the risk a rating, based on the severity of the impact and the likelihood of the risk occurring. This rating provides an easy to see colour code for how severe the risk could be to the privacy of individual and, therefore, the necessity of putting mitigating actions into place, or reassessing using the processing activity.

The risk rating table below uses the common 'Red, Amber, Green (RAG)' matrix, where each risk is given a RAG score, based on the likelihood versus the impact.

LIKELIHOOD	IMPACT					
		Trivial (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
	Almost Certain (5)	Low Med	Medium	High	Very High	Very High
	Likely (4)	Low	Low Med	Med High	High	Very High
	Possible (3)	Low	Low Med	Medium	Med High	High
	Unlikely (2)	Low	Low Med	Low Med	Medium	Med High
	Rare (1)	Low	Low	Low Med	Medium	Medium
Impact Score x Likelihood Score = Risk Rating						

- **GREEN** - Where an assessment outcome is green, the organisation still works to see if it can develop and implement any solutions or mitigating actions that can be applied to reduce the risk impact down as far as possible. However, most green rated risks are acceptable, and so focus should be placed on those with higher ratings. Even where a green RAG rating has been given at the risk/privacy identification stage, this risk is still to be added to the mitigating actions template for continuity, and to ensure that all risks have been recorded and assessed.

- **AMBER** - Where an assessment outcome is amber, mitigating actions are always proposed and outcomes envisaged, before processing is approved. The aim is to reduce all risks down to a green (*acceptable*) level. However, there will be occasions when processing must take place for legal/best interest reasons and so, some processing with risks will go ahead and must be accepted into the project. All solutions and mitigating actions must first be considered, tried and applied if possible.
- **RED** - Where an assessment outcome is red, it indicates that either or both impact and/or likelihood scores are unacceptable, and that complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level. Some processing activities are eliminated at this point as the impact to individuals is considered too high risk to proceed.

However, in instances where the activity is essential, or is a legal requirement, the proposed solutions and mitigating actions are applied and a further DPIA is completed to see if the subsequent DPIA results in a green and/or acceptable level of risk. If a high risk still exists and the processing activity is authorised, the Data Protection Officer will consult with the Supervisory Authority of the Data Protection Commissions Office prior to processing, and advise that the DPIA indicates that the processing would result in a high risk, and there is an absence of measures that can be taken mitigate the risk. The Data Protection Officer will await written advice from the Supervisory Authority and provide all information requested by them during this period.

The above process enables the organisation to devise ways to reduce or eliminate privacy risks, and assess the costs and benefits of each approach, as well as looking at the impact on an individual's privacy and the effect on the processing activity outcomes. This enables the organisation to document its identification and assessment of the risk, the solutions and mitigating actions used to reduce or eliminate the risk and records privacy risks, which have been accepted as necessary for the project to continue. Please refer to Appendix 1: Types of Privacy Risks and Appendix 2: Guidance for completing the Risk Register.

IDENTIFIED PRIVACY ISSUES AND ASSOCIATED RISKS					
REF	PRIVACY ISSUE	RAG	RISKS TO INDIVIDUAL(S)	COMPLIANCE RISK	CORPORATE RISK
#	<i>Use assessment response to detail the privacy factor resulting in risk</i>	<i>Risk Rating</i>	<i>Complete if risk impacts data subject(s) or put N/A if not applicable</i>	<i>Complete if risk causes non-compliance or put N/A if not applicable</i>	<i>Complete if risk impacts business or put N/A if not applicable</i>
PR1	<i>E.g. Processing relies solely on using automated systems</i>	8	<i>Affects rights under Article 22(1) Could result in biased results</i>	<i>Breaches Article 22(1)</i>	<i>Sanctions and fines for breaching GDPR</i>
PR2	<i>E.g. Processing makes it difficult to withdraw consent once given</i>	6	<i>Affects right to withdraw consent Unlawful processing</i>	<i>Breaches Article 7(3) Unlawful processing</i>	<i>Breach fines Reputational damage</i>

*Respect Service Collaboration Excellence Justice Creativity*

### 3.4 Identify and Evaluate Privacy Solutions:

Once all privacy issues and risks have been identified and rated, the organisation begins identifying and evaluating solutions and mitigating actions. The organisation addresses each issue and documents measures and controls that will reduce the risk impact. It is not possible to eliminate all risks, but the organisation aims to reduce them to an acceptable level. Where unable to reduce risks to this level, the organisation decides on cancelling the project or, accepting the risk if there is a legal/best interests' requirement.

It is the aim of the organisation to always to assess whether the impact on privacy is proportionate to the objectives of the project, and to ensure that individuals and their privacy remains its priority. The organisation considers any solution that may reduce risk and balance the aims with the impact.

When applying the solutions to the template, the organisation uses the risk rating obtained in the ***Risk Identification*** process to ensure that it knows the current risk and what an acceptable level would be. Once all solutions have been added, the organisation is then able to repeat the assessment of the risk and ascertain its eliminated, reduced or accepted result. The new risk rating is then added to the template.

***Some of the steps the organisation may use or consider to reduce risks include:***

- Changing the personal information collected to reduce the privacy level when processing.
- Carry out all processing in-house to avoid transfers or data sharing.
- Utilise systems/technology to make the processing more accessible.
- Creating new procedures for areas such as, retention, destruction methods, exercising rights.
- Developing new security measures for a specific project that align with its aims.
- Ensuring that adequate and effective training is provided to staff of the data protection regulations and the project processing.
- Publishing guidance manuals and supporting documents for use by those involved in the project.
- Creating new materials and website content to enable the organisation to better communicate with individuals.
- Carrying out higher level of due diligence on any processors used for the project.
- Producing data sharing agreements and transfer contracts.
- Having all involved in the project sign non-disclosure and confidentiality agreements.

The organisation also assesses the costs and benefits associated with all solutions to ensure that they are viable, feasible and proportionate to the privacy impact. All solutions also involve a review and input from the Data Protection Officer, who reviews them against the GDPR and any codes of conduct that the organisation follows, in accordance with data protection laws.

*Respect Service Collaboration Excellence Justice Creativity*

PROPOSED RISK SOLUTIONS AND MITIGATING ACTIONS						
REF	RISK	RAG	SOLUTION/MITIGATING ACTIONS	RESULT	OUTCOME	RAG
#	<i>Risk to be mitigated</i>	<i>Current rating</i>	<i>Detail corrective actions, solutions and mitigating controls that address the risk</i>	<i>Reduced, Eliminated or Accepted</i>	<i>Has the solution(s) reduced the risk enough to proceed with processing?</i>	<i>New risk rating</i>
PR1	<i>E.g. Processing relies solely on using automated systems</i>	8	<i>1. After processing completes, add human intervention stage to assess results for bias.</i> <i>2. Add system trigger to wait for human sign off</i>	<i>Risk Eliminated</i>	<i>Processing no longer relies solely on automated system as human intervention added, so risk is eliminated</i>	1
PR2	<i>E.g. Difficult to withdraw consent once given</i>	6	<i>Create communication to be sent to individual(s) with guidance for withdrawing consent in writing.</i>	<i>Withdrawal possible, but only in one format - Reduced</i>	<i>Due to type/location of processing, withdrawal of consent can only be done in writing. Can't offer opt-out or automated withdrawal options at this time</i>	6

*Respect Service Collaboration Excellence Justice Creativity*

### **3.5 Integrate Outcomes:**

Once all risks and privacy issues have been identified and mitigating actions and solutions applied to reduce, eliminate or accept the risks, making the project viable, the organisation then integrates the outcomes back into the project and creates an action plan for developing and implementing the solutions.

The integrated outcomes template enables the organisation to record what actions must now be taken to put the solutions identified above, into place. The organisation also details who has overall responsibility for ensuring that the actions are on track and completed, an estimated completion date and the status of the progress, so that any delays can be recorded and other parties can see how far along the organisation is in the process.

The action plan also allows the organisation to ensure that all risks and solutions have been accounted for, and are being mitigated against, and that no actions are missed or stalled. If at any point in the project, the objectives or processing operations change, or need to be amended, the organisation repeats the screening questions to ascertain if any new risks or privacy issues have been identified, and then add these to the DPIA and provide solutions and action plan for them also.

The screening questions and assessment questions are revisited after all actions are completed to ensure that they are still appropriate, and that solutions have reduced or eliminated the risks.

INTEGRATING OUTCOMES INTO PROJECT PLAN				
REF	ACTION(S) TO BE TAKEN	RESPONSIBILITY	COMPLETION DATE	PROGRESS/STATUS
#	<i>Details of what actions must happen for the solutions in the evaluation plan to be developed and implemented</i>	<i>Who is responsible for overseeing the actions and updating the project plan</i>	<i>What is the expected date that the actions will be completed</i>	<i>Current progress and/or action status</i>

*Respect   Service   Collaboration   Excellence   Justice   Creativity*

#### **4.0 Authorisation and Recording:**

All stages and aspects of a Data Protection Impact Assessment are recorded and retained for six years after the project implementation date. These are also used again should a similar project or technology be utilised in the future.

The stages in the DPIA aim to demonstrate that the organisation is carrying out effective assessments when high risks to privacy are involved, and that the security and privacy of personal data is one of its main priorities. Keeping records of all stages enables the organisation to evidence that it has identified, assessed and mitigated at every stage, and that all risks have been evaluated.

Where there is a requirement for the organisation to send a copy of the DPIA report to the Supervisory Authority, the Data Protection Officer will do this within the deadlines provided, and await their authorisation to proceed before going ahead with any processing. Such disclosures include the full report, along with a summary of the project, risks and proposed solutions.

The finalised DPIA is authorised by the Data Protection Officer, DPIA Lead and a Service Manager/Head of Department /Designate.

#### **DATA PROTECTION OFFICER:**

**Print Name:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**PIA Authorised:**     **Yes/No**     **Signed:** \_\_\_\_\_

#### **SERVICE MANAGER/HEAD OF DEPT/DESIGNATE:**

**Print Name:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**PIA Authorised:**     **Yes/No**     **Signed:** \_\_\_\_\_

**Review Date:** \_\_\_\_\_ **Signed:** \_\_\_\_\_  
**Data Protection Officer**

## **APPENDIX 1: TYPES OF PRIVACY RISK:**

### **Risks to individuals:**

- i. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- ii. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- iii. New surveillance methods may be an unjustified intrusion on their privacy.
- iv. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- v. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- vi. Identifiers might be collected and linked, which prevent people from using a service anonymously.
- vii. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- viii. Collecting information and linking identifiers might mean that an organisation is no longer using information, which is safely anonymised.
- ix. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- x. If a retention period is not established, information might be used for longer than necessary.

### **Examples of Compliance Risk:**

- i. Non-compliance with the common law duty of confidentiality.
- ii. Non-compliance with the Data Protection Acts 1988 & 2003/General Data Protection Regulation (GDPR).
- iii. Non-compliance with the Privacy and Electronic Communications Regulations (PECR)/e-Privacy Regulation.
- iv. Non-compliance with sector specific legislation or standards e.g. Health Information and Quality Authority (HIQA), Health and Safety Authority (HSA).
- v. Non-compliance with human rights legislation. United Nations Declaration on Human Rights (UNDHR).

### **Associated organisation/corporate risk:**

- i. Non-compliance with the Irish Data Protection Law or other legislation can lead to sanctions, fines and reputational damage.
- ii. Problems, which are only identified after the project has launched, are more likely to require expensive fixes.
- iii. The use of biometric information or potentially intrusive tracking technologies may cause increased concern, and cause people to avoid engaging with the organisation.
- iv. Information, which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- v. Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- vi. Data losses, which damage individuals, could lead to claims for compensation.

## **APPENDIX 2: GUIDANCE FOR COMPLETING A RISK REGISTER:**

- What is the actual risk? Make sure the risk is clear and concise, well understood and articulated, with appropriate use of language, suitable for the public domain.
- Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests. This is relevant if your organisation is subject to the FOI Act.
- Don't reference blame to other organisations in the risk register.
- Does the risk belong to a business area within your organisation or another body?

It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, and green. To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

### **Likelihood**

	Score				
Likelihood score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Frequency - how often might it happen?	This probably will never happen/recur	Do not expect it to happen/recur, but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur, but is not a persisting issue or circumstance	Almost certain to happen/recur; possibly frequently

### **Impact**

	Score				
Impact score	1	2	3	4	5
Descriptor	Very low	Low	Medium	High	Very high
Impact should it happen?	Unlikely to have any impact	May have an impact	Likely to have an impact	Highly probable it will have a significant impact	Will have a major impact

Using the risk “RAG” rating system for scoring risks means risks can be ranked, so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.

<b>Impact</b>	Very High - 5	A	A/R	R	R	R
	High - 4	A	A	A/R	R	R
	Medium - 3	A/G	A	A	A/R	A/R
	Low - 2	G	A/G	A/G	A	A
	Very Low - 1	G	G	G	G	G
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
		<b>Likelihood</b>				

*Respect Service Collaboration Excellence Justice Creativity*

### **APPENDIX 3: CHECKLIST FOR A DPIA:**

	<b>YES</b>	<b>NO</b>
1. Identify the need for a Data Protection Impact Assessment		
Is DPIA required?	<input type="checkbox"/>	<input type="checkbox"/>
2. Complete Project Brief and Plan.	<input type="checkbox"/>	<input type="checkbox"/>
3. Identify the privacy issues and associated risks.	<input type="checkbox"/>	<input type="checkbox"/>
4. Identify proposed risk solutions and mitigating actions.	<input type="checkbox"/>	<input type="checkbox"/>
5. Integrate outcomes into Project Plan.	<input type="checkbox"/>	<input type="checkbox"/>
6. Authorisation and Recording to include reporting the results to Senior Management Team or Supervisory Authority if required.	<input type="checkbox"/>	<input type="checkbox"/>
7. DPO and Project Lead will continue to monitor Project progress, and identify any new risks that need to be reflected in the DPIA.	<input type="checkbox"/>	<input type="checkbox"/>

## **10.0 AUDITS & MONITORING:**

### **10.1 Internal Compliance Audit:**

The Data Protection Officer has overall responsibility for the governance of Avista data management practices through the completion of annual audits and reviews across Avista, ensuring that outcomes of the audits are implemented within an agreed timeframe. The principle purpose on the internal audit is to ascertain whether Avista is operating in accordance with the Data Protection Acts and to take the corrective measures required.

The audit will be formulated around the Principles of the Data Protection Act and will include both manual and electronic data.

Ongoing support, training and development and policy development on data protection will be provided to promote continued awareness and understanding of all staffs' obligations under GDPR. This training will be reflected in the annual AVISTA training programmes across all regions.

The Data Protection Officer will provide reports on all audits and reviews to the Director of Governance, Planning and Strategy, the CEO on request, and members of the Senior Management/designate and local teams.

The Data Protection Officer will also make available to the Supervisory Authority audits and action plans when required.

### **10.2 External Compliance Audit:**

External Compliance Audits of all aspects of Data Protection within Avista may be conducted on a periodic basis by the Office of the Data Protection Commissioner. They may be scheduled in advance with Avista or unannounced.

### **10.3 Penalties:**

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

Adherence to the DOCS Data Protection Policy and Procedures and associated Data Management Policies is essential for all employees and third parties who access Avista personal and sensitive data to minimise enforcement of penalties. Avista recognises that:

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines which can be up to 4% of the total annual turnover of the preceding financial year.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country, or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to 4% of the total annual turnover of the preceding financial year.

*Respect Service Collaboration Excellence Justice Creativity*

## **11.0 REFERENCES:**

- General Data Protection Regulations May 2018 (GDPR).
- Data Protection Acts 1998 (The Primary Act).
- Data Protection (Amendment) Act 1988 & 2003.
- Electronic Communications Regulations 2011.
- Freedom of Information Acts 1997, 2003 & 2018.

## **12.0 REVIEW:**

The Data Protection Policy Avista DOCS 085 will be reviewed in accordance with changes to Legislation, Regulations and the Data Protection Acts.

## **13.0 APPENDICES:**

Appendix	1.1	Data Controller Agreement Template.
	1.2	Data Processor Agreement Template.
Appendix	2	Article 28 GDPR Requirement.
Appendix	3	GDPR It's Everyone's Responsibility/Clean Desk Guidelines.
Appendix	4.	Network Account Request Form.
	4.1	How to Encrypt a Document.
	4.2	Password Guidance for picking strong passwords.
Appendix	5	Easy to Read Privacy Statement for a Data Breach.

## **APPENDIX 1.1**

### **AVISTA**

#### **Joint Data Controller Agreement Template**

<b>Revision:</b>  <b>A</b>	<b>Department:</b>  <b>CEO</b>	<b>No:</b>  <b>DOCS 085</b>
<b>Prepared by:</b>	  _____ <b>Ms. Marie Grimes McGrath</b> <b>Data Protection Officer (DPO)</b>	<b>Date:</b>  <b>17/02/20</b>
<b>Approved by:</b>	  _____ <b>Ms. Natalya Jackson</b> <b>Chief Executive Officer (CEO)</b>	<b>Date:</b>

## Review History

No.	Old revision status	New Revision Status	Comment	Date	Prepared By	Approved by
1		A	Initial Issue	17/02/20	Marie Grimes McGrath	Natalya Jackson

## **DOCS 085 – Joint Data Controller Agreement Template**

<b>TABLE OF CONTENTS</b>	<b>Page</b>
1.0 Terms of Agreement	75
2.0 Definitions	75
3.0 Purpose	76
4.0 Compliance with National Data Protection Laws	76
5.0 Shared Personal Data	77
6.0 Fair and Lawful Processing	77
7.0 Data Quality	77
8.0 Data Subjects' Rights	77
9.0 Data Retention and Deletion	77
10.0 Security and Training	78
11.0 Data Security Breaches and Reporting Procedures	78
12.0 Resolution of Disputes with Data Subjects or The Data Protection Authority	79
13.0 Indemnity	79
14.0 Limitation of Liability	79
15.0 Term and Termination	79
16.0 Roles and Responsibilities	79

## JOINT DATA CONTROLLER AGREEMENT:

This joint data controller agreement for the sharing of Personal Data forms part of the **[insert contract name]** (“*Principal Contract*”) and is made effective from \_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_ *between* the undersigned parties:

(i) **[Controller Name]**, whose trading address is **[Controller Trading Address]** (“*Controller*”)

*And*

(ii) **[Controller Name]**, whose trading address is **[Controller Trading Address]** (“*Controller*”)

### 1.0 Terms of Agreement:

1.1 The following agreement between **[Controller Name]** and **[Controller Name]** reflects the arrangements that they have agreed to put in place to facilitate the sharing of Personal Data relating to **[insert as appropriate]** between the Parties acting as data controllers, and explains the purposes for which that Personal Data may be used. As such, **[Controller Name]** agrees to share the Personal Data with **[Controller Name]** on the terms set out in this Agreement and **[Controller Name]** agrees to use the Personal Data on the terms set out in this Agreement.

1.2 The terms used in this agreement have the meanings as set out in the 'definitions' part of the document.

### 2.0 Definitions:

2.1 In this Agreement, unless the text specifically notes otherwise, the below words shall have the following meanings:

2.2 “*Data Protection Laws*” means all applicable Data Protection Laws, including the General Data Protection Regulation (GDPR) (EU 2016/679) and, to the extent applicable, the data protection or privacy laws of any other country.

2.3 “*Data Controller*” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

2.4 “*EEA*” means the European Economic Area.

2.5 “*Effective Date*” means that date that this agreement comes into force.

2.6 “*Personal Data*” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.7 “*GDPR*” means the General Data Protection Regulation (GDPR) (EU) (2016/679).

2.8 “*Principal Contract*” means the main contract between the parties named in this agreement.

2.9 “*Processing*” means any operation or set of operations, which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.10 “*Data Discloser*” means the Party transferring the Personal Data to the Data Receiver.

2.11 “*Data Receiver*” means the Party receiving the Personal Data from the Data Discloser.

2.12 “*Supervisory authority*” means an independent public authority which is established by a Member State pursuant to Article 51 of the “GDPR”.

*Respect Service Collaboration Excellence Justice Creativity*

### **3.0 Purpose:**

#### **3.1** Article 26 of the GDPR sets out the following in respect of Joint Data Controllers:

*“1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.*

*2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.*

*3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.”*

#### **3.2** This Agreement sets out the framework for the sharing of personal data between the parties as Data Controllers and defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

#### **3.3** The sharing of personal data is necessary to support the following agreed purposes of both parties: **[Insert as appropriate]**

#### **3.4** The parties agree that this Agreement formalises a lawful transfer of personal data between the parties and presents no new or additional privacy concerns. A Data Privacy Risk Assessment has been conducted in respect of the personal data to be shared and the necessity of the sharing; this Agreement serves to address any residual privacy or information risks and document the actions taken to identify, address and mitigate those risks wherever possible.

#### **3.5** The parties shall not process shared personal data in a way that is incompatible with the agreed purposes.

### **4.0 Compliance with National Data Protection Laws:**

#### **4.1** Each party must ensure compliance with applicable national data protection laws at all times during the Term.

**5.0 Shared Personal Data:**

**5.1** The following types of personal data may be shared between the parties during the term:

**[Insert as appropriate]**

**5.2** The shared personal data must not be irrelevant or excessive with regard to the agreed purposes.

**6.0 Fair and Lawful Processing:**

**6.1** Each party shall ensure that it processes the shared personal data fairly and lawfully in accordance with applicable legislation during the term of this Agreement.

**6.2** For the purposes of agreed purposes as listed in clause 3.3 of this Agreement, each party shall ensure that it processes shared personal data on the basis of one of the following legal grounds:

**[Insert lawful condition for processing, per Article 6, Article 9, Article 10, Article 11 of the GDPR as appropriate]**

**6.3** Both parties shall, in respect of shared personal data, ensure that their privacy notices are clear and provide sufficient information to data subjects in order for them to understand what of their personal data the parties are sharing, the circumstances in which it will be shared, the purposes for the data sharing, and either the identity with whom the data is shared, or a description of the type of organisation that will receive the personal data.

**6.4** Both parties undertake to inform data subjects of the purposes for which it will process their personal data and provide all of the information that it must provide in accordance with its own applicable laws, to ensure that the data subjects understand how their personal data will be processed by the Data Controller.

**7.0 Data Quality:**

**7.1** The Data Discloser shall ensure that shared personal data is accurate.

**7.2** Where either party becomes aware of inaccuracies in shared personal data, they will notify the other party.

**7.3** Shared personal data shall be limited to the personal data described in clause 5.1 of this Agreement.

**8.0 Data Subjects' Rights:**

**8.1** Data subjects have the right to obtain certain information about the processing of their personal data through a Subject Access Request. Data subjects may also request rectification, erasure or blocking of their personal data.

**8.2** The parties shall maintain a record of Subject Access Requests, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.

**8.3** The parties agree that the responsibility for complying with a Subject Access Request falls to party receiving the Subject Access Request in respect of the personal data held by that party.

**8.4** The parties agree to provide reasonable and prompt assistance (within 5 Business Days of such a request for assistance) as is necessary to each other, to enable them to comply with Subject Access Requests, and to respond to any other queries or complaints from data subjects.

**9.0 Data Retention and Deletion:**

**9.1** The Data Receiver shall not retain or process shared personal data for longer than is necessary to carry out the agreed purposes.

**9.2** Notwithstanding clause 9.1, the parties shall continue to retain shared personal data in accordance with any statutory or professional retention periods applicable in their respective countries and/or industry.

*Respect Service Collaboration Excellence Justice Creativity*

- 9.3** The Data Receiver shall ensure that any shared personal data is returned to the Data Discloser or destroyed in the following circumstances:
- On termination of the Agreement for whatever reason.
  - On expiry of the term (unless extended further to the terms of this Agreement).
  - Once processing of the shared personal data is no longer necessary for the purposes it was originally shared for.

**10.0 Security and Training:**

- 10.1** The Data Discloser shall be responsible for the security of transmission of any shared personal data in transmission to the Data Receiver by using appropriate technical methods. These are detailed below:

**[Name of controller]** will only share shared personal data in compliance with its encryption guidelines (a copy of the current version can be found via the following link: **[Insert as appropriate]**).

- 10.2** The parties agree to implement appropriate technical and organisational measures to protect the shared personal data in their possession against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, including but not limited to:

- Ensuring IT equipment, including portable equipment is kept in lockable areas when unattended.
- Not leaving portable equipment containing the personal data unattended.
- Ensuring that staff use appropriate secure passwords for logging into systems or databases containing the personal data.
- Ensuring that all IT equipment is protected by antivirus software, firewalls, passwords and suitable encryption devices.
- In particular, ensure that any sensitive personal data is stored and transferred (including where stored or transferred on portable devices or removable media), using industry standard 256-bit AES encryption or suitable equivalent.
- Limiting access to relevant databases and systems to those of its officers, staff agents and sub-contractors, who need to have access to the personal data, and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged by the party.
- Conducting regular threat assessment or penetration testing on systems.
- Ensuring all staff handling personal data have been made aware of their responsibilities with regards to handling of personal data.
- Allowing for inspections and assessments to be undertaken by the other party in respect of the security measures taken, or producing evidence of those measures if requested.

**11.0 Data Security Breaches and Reporting Procedures:**

- 11.1** The parties are under a strict obligation to notify any potential or actual losses of the shared personal data to the other party as soon as possible and, in any event, within one business day of identification of any potential or actual loss, to enable the parties to consider what action is required in order to resolve the issue, in accordance with the applicable national data protection laws and guidance.
- 11.2** Clause 11.1 also applies to any breaches of security, which may compromise the security of the shared personal data.
- 11.3** The parties agree to provide reasonable assistance as is necessary to each other, to facilitate the handling of any data security breach in an expeditious and compliant manner.

*Respect Service Collaboration Excellence Justice Creativity*

**12.0 Resolution of Disputes with Data Subjects or the Data Protection Authority:**

- 12.1** In the event of a dispute or claim brought by a data subject or the Data Protection Authority concerning the processing of shared personal data against either or both parties, the parties will inform each other about any such disputes or claims, and will co-operate with a view to settling them amicably in a timely fashion.
- 12.2** The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the Data Protection Authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
- 12.3** In respect of breaches relating to this Agreement, each party shall abide by a decision of a competent court of the Data Discloser's country of establishment, or of any binding decision of the relevant Data Protection Authority.

**13.0 Indemnity:**

**[Insert indemnity clause as appropriate].**

**14.0 Limitation of Liability:**

**[Insert limitation of liability clause as appropriate].**

**15.0 Term and Termination:**

- 15.1** This Agreement shall commence on [Insert date] and shall continue in force for the **[remainder of the]** Term.
- 15.2** The Agreement shall automatically terminate on expiry of the term unless, following a review of the terms of the Agreement, the parties agree to extend the Agreement for a further **[Insert duration]**.
- 15.3** Any such renewal shall be in writing signed by an authorised signatory of both parties and the parties shall seek to agree any such renewal at least **[Insert]** months in advance of the expiry of the Term.

**16.0 Roles and Responsibilities:**

- 16.1** Each party shall nominate a single point of contact within their organisation, who can be contacted in respect of queries or complaints regarding the DPA, GDPR and/or compliance under the terms of this Agreement.  
**[Insert relevant details here]**

**Signed on behalf of the Joint Data Controller:**

Signed: \_\_\_\_\_

Print Name: \_\_\_\_\_

Date: \_\_\_\_\_

Company Name: \_\_\_\_\_

Position: \_\_\_\_\_

*Respect Service Collaboration Excellence Justice Creativity*

**Signed on behalf of the Joint Data Controller:**

Signed: \_\_\_\_\_

Print Name: \_\_\_\_\_

Date: \_\_\_\_\_

Company Name: \_\_\_\_\_

Position: \_\_\_\_\_

## **APPENDIX 1.2**

### **AVISTA**

#### **Data Processor Agreement with \_\_\_\_\_ (Template)**

<b>Revision:</b> <b>A</b>	<b>Department:</b> <b>CEO</b>	<b>No:</b> <b>DOCS 085</b>
<b>Prepared by:</b>	  _____ <b>Marie Grimes McGrath</b> <b>Data Protection Officer (DPO)</b>	<b>Date:</b> <b>14/10/19</b>
<b>Approved by:</b>	  _____ <b>Natalya Jackson</b> <b>Chief Executive Officer (CEO)</b>	<b>Date:</b> <b>14/10/19</b>

#### **Review History**

<b>No.</b>	<b>Old revision status</b>	<b>New Revision Status</b>	<b>Comment</b>	<b>Date</b>	<b>Prepared By</b>	<b>Approved by</b>
1		A	Initial Issue	14/10/19	Marie Grimes McGrath	Natalya Jackson

## **DOCS 085 – Data Processor Agreement Template**

<b>TABLE OF CONTENTS</b>	<b>Page</b>
An Agreement with	82
Recitals	82
1.0 Agreement	84
2.0 Obligations of the Data Controller	84
3.0 Obligations of the Data Processor	84
4.0 Right of Audit	86
5.0 Data Subject Rights	86
6.0 Indemnities	87
7.0 Governing Law	88
Data Processor Contract Evaluation	89
Data of Contract Evaluation	90

## AN AGREEMENT BETWEEN:

- (1) [ **Data Controller name**]  
Established at [Registered Address] - “**the Data Controller**”;  
and
- (2) [ **Data Processor name**]  
Established at [Registered Address] - “**the Data Processor**”

## RECITALS

- (A) Under the Irish Data Protection legislation, a written Agreement must be in place between the Data Controller and any organisation which processes personal data on its behalf, governing the processing of that data. This Agreement is intended to satisfy that obligation.
- (B) The Data Controller is engaging the services of the Data Processor as its agent for the purpose of providing the following data management services– “**The Services**”
- [description of intended data processing]
  - [description of intended data processing]
  - [description of intended data processing]
- The subject-matter and the nature of the processing will include:
- [description of the subject-matter and the nature of processing here]
  - [description of the subject-matter and the nature of processing here]
  - [description of the subject-matter and the nature of processing here]
- (C) The Data Processor agrees to process the personal data strictly within the defined length of time agreed between the Data Controller and the Data Processor. This length of time will be [agreed contract duration].
- (D) The Data Controller and the Data Processor have agreed that the type(s) of personal data being processed will be:
- [insert description of the type of personal data here]
  - [insert description of the type of personal data here]
  - [insert description of the type of personal data here]
- And, where relevant, the following categories of Sensitive Personal Data:
- [insert description of the type of sensitive personal data here]
  - [insert description of the type of sensitive personal data here]
  - [insert description of the type of sensitive personal data here]
- (E) The Data Controller shall authorise the Data Processor to process the data in any manner that may reasonably be required in order for the Data Processor to carry out the processing in compliance with this Data Processor Agreement.
- (F) The Data Controller shall refrain from providing instructions, which are not in accordance with applicable laws and, in the event that such instructions are given, the Data Processor is entitled to resist carrying out such instructions.

*Respect Service Collaboration Excellence Justice Creativity*

(G) The parties now wish to enter into this Agreement in order to regulate the provision, use and processing of Personal Data which the Data Processor will be processing on behalf of the Data Controller.

(H) The terms referred to in this Agreement will be used as they are used in applicable laws or, if not inconsistent with these laws, in accepted general principles and practices. Specifically, the terms “Data Controller”, “Data Processor”, “Data Subject”, “Personal Data”, “Sensitive Personal Data” and “Processing” shall be defined as by applicable data protection legislation.

**1.0 Agreement:**

**1.1** This Agreement shall continue in full force for the duration stated, unless terminated for breach by either party.

**2.0 Obligations of the Data Controller:**

**2.1** The Data Controller shall authorise the Data Processor to process the personal data in any manner that may reasonably be required in order to provide the services.

**2.2** The instructions given by the Data Controller to the Data Processor in respect of the personal data shall at all times be in accordance with the laws of Ireland.

**2.3** [Include further, specific obligations of the Data Controller, as appropriate].

**3.0 Obligations of the Data Processor:**

**3.1** In discharging its obligations under this Agreement, the Data Processor must comply with all applicable law, in particular data protection regulations. In particular, the Data Processor will ensure that all necessary logging, registrations and notifications are made, and will co-operate with the Data Controller in relation to evidential matters, amendments or alterations.

**3.2** The Data Processor undertakes that he shall only process the personal data on documented instructions from the Data Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by applicable law to which the Data Processor is subject.

In such a case, the Data Processor undertakes to inform the Data Controller of that legal requirement before processing takes place, unless that law prohibits such information on important grounds of public interest.

“Third country” or “international organisation” in this context means a destination outside the European Economic Area.

**3.3** The Data Processor will process the Personal Data for the following purposes only:

- [Purpose]
- [Purpose]

**3.4** The Data Processor agrees to execute its obligations in this contract using the following process:

- [Process]
- [Process]

**3.5** The Data Processor will treat the personal data and any other information provided by the Data Controller as confidential, and will ensure that access to the personal data is limited only to authorised persons who require to access it for the purposes defined in this Agreement.

The Data Processor will ensure that persons authorised to process the personal data have committed themselves to confidentiality, or are under an appropriate statutory obligation of confidentiality.

*Respect Service Collaboration Excellence Justice Creativity*

In this context, the Data Processor will ensure that all such authorised persons have undergone the required training to discharge the obligation to uphold confidentiality as required by applicable laws.

The Data Processor will not disclose any personal data to a third party in any circumstances, other than at the specific written request of the Data Controller, unless such disclosure is necessary in order to deliver the services, or is required by applicable legislation.

- 3.6** The Data Processor undertakes to implement the appropriate organisational and technological measures in such a manner that meet the requirements of applicable law, in particular relevant data protection legislation, in order to ensure the protection of the rights of the data subjects.
- 3.7** The Data Processor will not transfer the personal data to a destination outside the European Economic Area (EEA), other than at the specific written request of the Data Controller, unless the transfer is required by law.
- 3.8** The Data Processor shall not engage another processor without the prior specific written authorisation of the Data Controller. The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other processors before such changes are effected, thereby giving the controller the opportunity to object to such changes. (Amend as appropriate).

Where engaging a sub-contractor, the Data Processor will obtain guarantees from such other processor that he will implement organisational, operational and technological processes and procedures in compliance with the principles of appropriate standards and all applicable laws, and will use such principles and laws as the basis for discharging his obligations in this regard.

- 3.9** The Data Processor will implement appropriate technical and organisational measures to ensure a level of security appropriate to identified risks, including inter alia as appropriate:
- The pseudonymisation and encryption of personal data.
  - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
  - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
  - Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

In assessing the appropriate level of security, the Data Processor will implement all reasonable measures to keep the personal data safe from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

- 3.10** The Data Processor will notify the Data Controller as soon as possible once becoming aware of a personal data breach. The Data Processor will co-operate with the Data Controller in implementing any appropriate action concerning the breach, including corrective actions, unless such action is contrary to applicable law.
- 3.11** In the event that the Data Processor receives a complaint, notice or communication, which relates directly or indirectly to the processing of the data or other connected activities, or which relates directly or indirectly to the compliance of the Data Processor, the Data Controller or other involved parties with relevant laws and relevant data protection legislation, the Data Processor will immediately bring this complaint, notice or communication to the attention of the Data Controller.

*Respect Service Collaboration Excellence Justice Creativity*

- 3.12** The Data Processor will assist the Data Controller to delete or return all the personal data to the Data Controller after the end of the provision of services relating to processing, and deletes existing copies available, unless the instruction of the Data Controller conflicts with applicable legislation on the continued retention and storage of such data.

The Data Processor shall not delete or return to the Data Controller any data without the prior written notification for same, allowing the Data Controller reasonable time to object to such deletion or return, even upon the termination, discharge or conclusion of this agreement or the processing activity, as the case may be.

- 3.13** Without prejudice to other legal provisions concerning the data subject's right to compensation and liability of the parties generally, as well as legal provisions concerning fines and penalties, the Data Processor will carry full liability in the instance where he is found to have infringed applicable laws, including data protection regulations, by determining the purposes and means of processing.

#### **4.0 Right of Audit:**

- 4.1** The Data Processor will allow for, and contribute to audits, including inspections, which may be carried out by the Data Controller or another auditor mandated by the Data Controller.
- 4.2** In the event that the Data Processor forms the opinion that the instruction of the Data Controller infringes applicable law, he/they will immediately inform the Data Controller.
- 4.3** The Data Controller is entitled to carry out carry out compliance and information security audits [without notice/with notice of (insert notice period)] (delete as appropriate) [during business hours/at any time of the day] (delete as appropriate), in order to satisfy itself that the Data Processor is adhering to the terms of this agreement.
- 4.4** The Data Controller may make a written request, or request in the course of an audit or inspection, for a copy of all data and data-related activity logs from the Data Processor and such information shall be provided by the Data Processor without unreasonable delay in the format, and on media as reasonably specified by the Data Controller.
- 4.5** Where a sub-contractor has been engaged, the Data Processor agrees that the Data Controller may also, upon giving reasonable notice and within normal business hours, carry out similar compliance and information security audits and checks of the sub-contractor to ensure adherence to the terms of this agreement.

#### **5.0 Data Subject Rights:**

- 5.1** The Data Processor will assist the Data Controller, whenever reasonably required, in so far as possible, to fulfil the Data Controller's obligation to respond to requests for exercising the Data Subject's rights as provided by relevant legislation.

In doing so, both the Data Controller and the Data Processor will take into account the nature of the processing and the appropriate technical and organisational measures, which have been implemented.

- 5.2** The Data Processor will assist the Data Controller in ensuring compliance with its legal obligations as provided by applicable legislation, in particular data protection legislation, concerning the security of processing, the notification requirements to relevant authorities, the requirement to communicate personal data breaches to the data subject, the requirement to carry out data protection impact assessments, and the requirement to consult with relevant authorities concerning high-risk processing prior to carrying out such processing. In discharging this obligation, the Data Processor may have regard to the nature of the processing and the information available to him.

*Respect Service Collaboration Excellence Justice Creativity*

The Data Processor will make all the information necessary to demonstrate compliance with the obligations by applicable law, in particular applicable data protection legislation.

**5.3** The data subject is hereby entitled to enforce the terms and conditions of this Agreement as a third-party beneficiary.

**6.0 Indemnities:**

Each party shall indemnify the other against all costs, expense, including legal expenses, damages, loss, including loss of business or loss of profits, liabilities, demands, claims, actions or proceedings which a party may incur arising out of any breach of this Agreement howsoever arising for which the other party may be liable.

**7.0 Governing Law:**

This Agreement shall be governed by and construed in accordance with Irish law and each party hereby submits to the non-exclusive jurisdiction of the Irish courts.

Signed..... Date.....

on behalf of [Data Controller Name] - the Data Controller

Signed..... Date.....

on behalf of [Data Processor Name] - the Data Processor

## **Data Processor Contract Evaluation**

Within the provisions of the GDPR, Article 28.3 sets out that:

*“Processing [of personal data] by a Processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the Processor with regard to the Controller and that sets out the subject-matter and duration of the processing...”*

Furthermore, Article 28.4 requires that:

*“Where a Processor engages another Processor (Sub-Contractor) for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the contract or other legal act between the Controller and the Processor ... shall be imposed on that (sub-contractor) by way of a contract ..., in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation.*

*Where that (sub-contractor) fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that (sub-contractor)'s obligations.”*

The purpose of this document is to help organisations to evaluate existing and new contracts to ensure that they meet these requirements prior to the enforcement date of the GDPR, May 25th, 2018.

### **Parties to the Contract:**

<b><u>Data Controller</u></b>	<b><u>Data Processor</u></b>

**OR**

<b><u>Data Processor</u></b>	<b><u>Sub-Contractor</u></b>

**OR**

<b><u>Lead Data Controller</u></b>	<b><u>Joint Data Controller</u></b>

**Data of Contract Evaluation:** \_\_\_\_\_

*Respect   Service   Collaboration   Excellence   Justice   Creativity*

<b>GDPR Requirement</b>	<b>Incorporated within Contract?</b> <i>[Where existing, please reference Clause and Paragraph]</i>
A description or outline of the subject-matter of the intended processing:	
The duration of the processing:	<b>From:</b>  <b>To:</b>
A description of the nature and purpose of the processing:	
A description of categories/type(s) of personal data involved – e.g. whether personal data or sensitive data (ethnic, religious, political/ideological, medical, trade union, sexual orientation, criminal):	
A description of categories of data subjects whose personal data will be processed – employees, customers, residents, patients, students, donors, marketing ‘leads’, etc.	
The obligations and rights of the Controller, e.g. parameters for processing, or constraints imposed on the activities of the Processor during the contract term:	
A commitment that the Processor will only process the personal data based on documented instructions from the Controller:	
A clear statement that the Processor will ensure that persons authorised by the Processor to process the personal data have committed themselves to protecting the confidentiality of that data:	
A commitment that the Processor will take all appropriate measures required to ensure the security of the personal data (with regard to Article 32 of the GDPR):	
Confirmation that the Processor will respect the preferences of the Data Controller with regard to engaging another Processor or Sub-Contractor	

An undertaking that the Processor will assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation in responding to requests relating to a Data Subject's rights:	
A commitment that the Processor will assist the Controller in ensuring compliance with the obligations regarding data security, in as far as possible:	
Consistent with the preferences of the Controller, a commitment that the Processor will delete or return all the Personal Data to the Controller after the end of the provision of services outlined in the contract:	
An undertaking that the Processor will make available to the Controller all information necessary to demonstrate compliance with the obligations set out in the GDPR, and will allow for and contribute appropriately to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller:	

## **APPENDIX 2**

<b>Article 28 GDPR requirement</b>	<b>Y</b>	<b>N</b>
The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures to protect the data.		
The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors.		
The processor must ensure that any relationship with a sub-processor contains similar clauses as contained within this agreement.		
<b><i>Contract must include...</i></b>		
- the subject-matter of the processing	-	-
- the duration of the processing	-	-
- the nature of the processing	-	-
- the purpose of the processing	-	-
- the type of personal data	-	-
- the categories of data subjects	-	-
- the obligations and rights of the controller	-	-
<b><i>Processor must...</i></b>		
- process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation	-	-
- ensure that persons authorised to process the personal data have committed themselves to confidentiality	-	-
- take all measures required pursuant to Article 32 (Security of processing)	-	-
- assist the controller for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights (per Articles 12 – 23)	-	-
- assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36	-	-
- delete/ return all the personal data to the controller after the end of the provision of services (unless retention is required by law)	-	-
- make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections	-	-
- immediately inform the controller if, in its opinion, an instruction infringes GDPR	-	-

### **APPENDIX 3: DATA PROTECTION ‘IT’S EVERYONE’S RESPONSIBILITY’**

Please refer to these practical guidelines to assist staff to promote safe and secure data management practices to ensure the organisation’s compliance with the General Data Protection Regulations.

#### **GDPR – IT’S EVERYONE’S RESPONSIBILITY:**

Avista must comply with all applicable data protection, privacy and security laws and regulations in the locations in which the organisation operates. In the course of the organisation’s work, staff are required to collect and use certain types of information about people (hereafter referred to as data subjects in line with the regulation) including ‘personal data’ and ‘special category data’ as defined also by the General Data Protection Regulation. This information can relate to service users, current, past and prospective employees, suppliers and others with whom staff communicate. In addition, staff may occasionally be required to collect and use certain types of personal information and/or special categories of personal data to comply with the requirements of other legislation, for example, infectious diseases legislation. Avista has a responsibility to ensure that this personal data is:

- Obtained fairly.
- Recorded correctly, kept accurate and up-to-date.
- Used and shared both appropriately and legally.
- Stored securely.
- Not disclosed to unauthorised third parties.
- Disposed of appropriately (in line with Avista DOCS 050 Records Management Policy).

All staff working in Avista are legally required under EU and Irish legislation to ensure the security and confidentiality of all personal data they collect and process on behalf of service users and employees. Data Protection rights apply, whether the personal data is held in electronic format or in a manual or paper-based form. Staff breaches of data protection regulation may result in disciplinary action.

Compliance with Data Protection Legislation has been included in the Service Level Agreements signed by the CEO and ACEOs of the various regions.

#### **Take These Practical Steps to Protect Data and Patient Privacy/Clear Desk Guidelines:**

##### ***Personal information should not be deliberately or inadvertently viewed by uninvolved parties.***

- Staff should operate clear desk guidelines at the end of each working day and when away from the desk or the office for long periods.
  - Personal and sensitive records held on paper and/or on screens must be kept hidden from callers to offices/stations/public hatches.
  - Records (service user or staff files) containing personal information must never be left unattended where they are visible, or maybe accessed by unauthorised staff or members of the public.
  - If computers or VDUs are left unattended, staff must ensure that no personal information may be observed or accessed by unauthorised staff or members of the public.
  - The use of secured screen savers is advised to reduce the chance of casual observation.
  - Rooms, cabinets or drawers in which personal records are stored should be locked when unattended. A record tracing system should be maintained of files removed and/or returned.
- It is important to ensure that service user and/or staff information is not discussed in inappropriate areas, where it is likely to be overheard, including conversations and telephone calls. Particular care should be taken in areas where the public have access.

*Respect Service Collaboration Excellence Justice Creativity*

While appreciating the need for information to be accessible, staff must ensure that personal records are not left on desks or workstations at times when unauthorised access might take place.

- Staff must only access service user information on a need to know basis, and should only view or share data that is relevant or necessary for them to carry out their duties.

***Do not leave information/data unattended in cars:***

- Staff must not leave laptops/portable electronic devices and/or files containing personal information unattended in cars.
- In cases where staff removes files/records from offices to attend meetings, home visits etc. the records should always be contained in a suitable brief case/bag to avoid any inappropriate viewing and also to secure the records. Where files are removed from an area, there should be a Log-In/Log-Out internal file system for the area to track and monitor the life cycle of the file.
- All files and portable equipment must be stored securely. If files containing personal information must be transported in a car, they should be locked securely in the boot for the minimum period necessary.
- Staff should not take records home. However, in exceptional cases, where this cannot be avoided the records must be stored securely. Records should not be left in a car overnight, but stored securely indoors.

***Transmitting information by Fax or Post:***

Staff must respect the privacy of others at all times and only access fax messages where they are the intended recipient or they have a valid work-related reason.

If a staff member receives a fax message and they are not the intended recipient, they must contact the sender and notify them of the error.

Fax machines must be physically secured and positioned to minimise the risk of unauthorised individuals accessing the equipment or viewing incoming messages.

Where possible the information should be encrypted and transmitted via email.

It is acceptable to transmit confidential and personal information by fax only when:

1. All persons identified in the fax message have fully understood the risks and agreed.
2. There are no other means available.
3. In a medical emergency, where a delay would cause harm.

The following steps are to be taken to maintain security and confidentiality when transmitting personal information by fax:

- The fax message must include an Avista Fax Cover Sheet.
- Only the minimum amount of information necessary should be included in the fax message.
- Before sending the fax message, contact the intended recipient to ensure he/she is available to receive the fax at an agreed time.
- Ensure that the correct number is dialled.
- Keep a copy of the transmission slip and confirm receipt of the fax message.
- Ensure that no copies of the fax message are left on the fax machine.

*Respect Service Collaboration Excellence Justice Creativity*

When using the postal system, mail containing sensitive personal information should be marked clearly with "Strictly Private and Confidential". If proof of delivery is necessary, information of this nature should be sent by registered post. Please also provide "return to sender" information in the event that the mail is undeliverable.

***Staff must adhere to Avista' Password Standards Policy:***

All passwords must be unique and must be a minimum of 8 characters. If existing systems are not capable of supporting 8 characters, then the maximum number of characters allowed must be used.

Passwords must contain a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: “, £, \$, %, ^, &, \*, @, #, ?, !, €).

**Passwords must not be left blank:**

Users must ensure passwords assigned to them are kept confidential at all times and are not shared with others including co-workers or third parties. In exceptional circumstances, where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others. For full details please refer to Avista **Password Policy**.

***Staff must adhere to Avista DOCS 014 Information Technology, Email and Internet Policy:***

Confidential and personal information stored on shared AVISTA network servers, which are situated in physically unsecure locations, for example, remote file/print servers, must be protected by the use of strict access controls and encryption. All devices used for the storage and processing of personal data must be encrypted. It is the responsibility of each device owner to ensure that the device is appropriately secure.

- Where possible all confidential and personal information must be stored on a secure Avista network server with restricted access. Where it has been deemed necessary by the information owner to store confidential or personal information on any device other than an Avista network server, the information must be encrypted.
- Avista desktop computers, which for business or technical reasons need to store/host AVISTA service user or employee information systems and/or confidential or personal information locally (as opposed to a secure Avista network server) must have Avista approved encryption software installed.
- Avista desktop computers used by employees to work from home (home working) must have Avista approved encryption software installed.
- All Avista laptop computer devices must have Avista approved encryption software installed prior to their use within Avista. In addition to encryption software, the laptop must be password protected, and have up to date anti-virus software installed.
- Only Avista approved USB memory sticks, which are distributed by the IT Administrator may be used to store or transfer Avista data. Avista IT security policies specifically prohibit the storage of AVISTA data on unapproved encrypted/unencrypted USB memory sticks and USB memory sticks, which are the personal property of staff and are not owned or leased by Avista.
- Avista approved USB memory sticks must only be used on an exceptional basis, where it is essential to store or temporarily transfer confidential or personal data. They must not be used for the long-term storage of confidential and personal data, which must, where possible, be stored on a secure Avista network server.
- Specific services or areas may take local decisions to prohibit completely the use of encrypted USB memory sticks to store personal data.

***Mobile Phones:***

*Respect Service Collaboration Excellence Justice Creativity*

- Users must ensure their Avista mobile phone device is protected at all times.
- At a minimum, all mobile phone devices must be protected by the use of a Personal Identification Number (PIN). The mobile phone device must be password protected and all passwords must meet the requirements of **Avista Password Records System**.
- Users must take all reasonable steps to prevent damage or loss to their mobile phone device. This includes not leaving it in view in an unattended vehicle and storing it securely when not in use. The user may be held responsible for any loss or damage to the mobile phone device, if it is found that reasonable precautions were not taken.
- Confidential and personal information must not be stored on an Avista mobile phone device without the prior authorisation of Avista information owner. Where confidential and personal information is stored on a Avista mobile phone device, the information must be encrypted in accordance with Avista Encryption Guidelines.
- Users must respect the privacy of others at all times, and not attempt to access Avista mobile phone device calls, text messages, voice mail messages or any other information stored on a mobile phone device, unless the assigned user of the device has granted them access.
- Mobile phone devices equipped with cameras must not be used inappropriately within Avista.
- Confidential and/or personal information regarding Avista, its employees or service users must not be sent by text message.
- All email messages sent from a Avista mobile phone device, which contains confidential and/or personal information must be sent and encrypted in accordance with Avista Electronic Communications Policy.
- Users must report all lost or stolen mobile phone devices to their Line Manager, the Data Protection Officer and the IT Administrator immediately.
- If a lost or stolen Avista mobile phone device contained confidential or personal information, this must be reported and managed in accordance with Avista Data Protection Breach Management Policy.

## **APPENDIX 4.**



Network Account Request Form

**Author:** Avista

**Revision Date:** 01/05/2019

**Version:** V1.0

### Network Account Request Form

#### **Employee Information:**

Employee First Name   
Employee Middle Name   
Employee Surname   
Cost Centre Code   
Activation Date

**Equipment Required:**

PC ☐ Laptop ☐ Tablet ☐ Desk Phone ☐ Encrypted USB stick ☐ Swipe Access card\Fob ☐

If Mobile Phone: Talk & Text ☐ Smartphone ☐ Mobile Wi-Fi ☐

**Network Shared Folder Access:** Yes ☐ No ☐

If Yes, please list the required shared folders (Note correct drive names required):


Name of Requestor:

Date:

Copyright © 2019 | Avista

Network Account Request Form

**Author:** Avista

*Respect Service Collaboration Excellence Justice Creativity*

Network Account Closure Form

**Account Information:**

Employee Account Name   
Cost Centre Code   
De-Activation Date

**Equipment to be returned:**

PC ☐ Laptop ☐ Tablet ☐ Desk Phone ☐ Encrypted USB stick ☐ Swipe Access card\Fob  
☐ If Mobile Phone: Talk & Text ☐ Smartphone ☐ Mobile Wi-Fi ☐

**Network Shared Folder Access will be removed from the account.**

Has e-mail account contents been cleared and all Avista information been copied to appropriate shared folders/ECRS/MIS Yes ☐ No ☐

If no who has been designated to do this work?

Has the Employees home folder been cleared? Yes ☐ No ☐

Has the Employee's Password Encryption Registered been received by Manager? Yes ☐ No ☐

If no please explain?

I confirm that Avista data created has been filed appropriately

Signature of Employee:

Employee Manager:

Date:

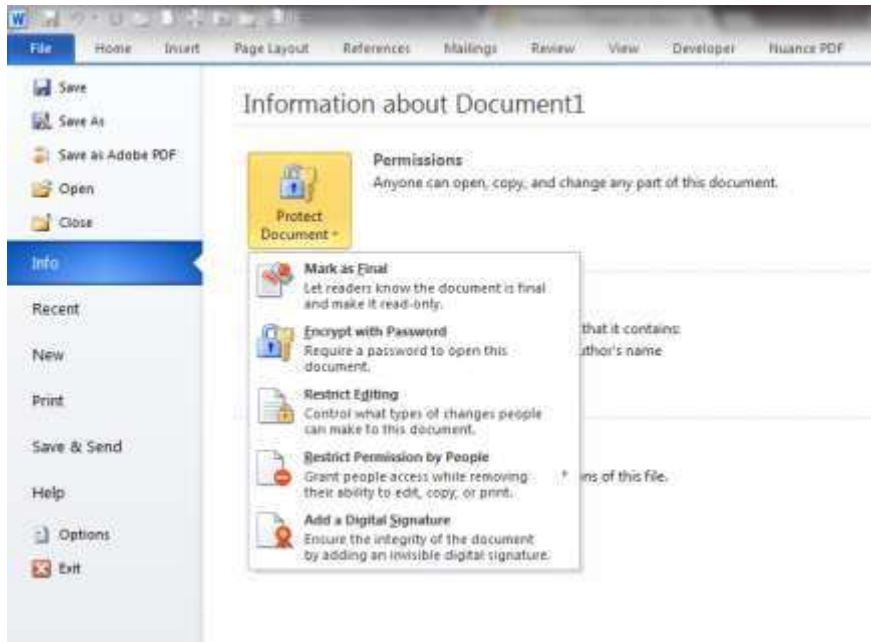
Copyright © 2019 | Avista

## **APPENDIX 4.1**

## **HOW TO ENCRYPT A DOCUMENT**

### **How to Encrypt a Word Document**

Open the document you want to encrypt. Go to File, and select Info and select protect document. From the drop-down menu select Encrypt with Password.



Next dialogue box to open is the password box. Note you should enter a strong password – it should contain capital letter/s, lowercase letter/s, number and a symbol such as !+\*%\*. Remember once this is entered you or anyone else will not be able to access the document without the password. Create a separate word document to record the password, date, recipient and password used and store it in your home folder (O:/ drive):



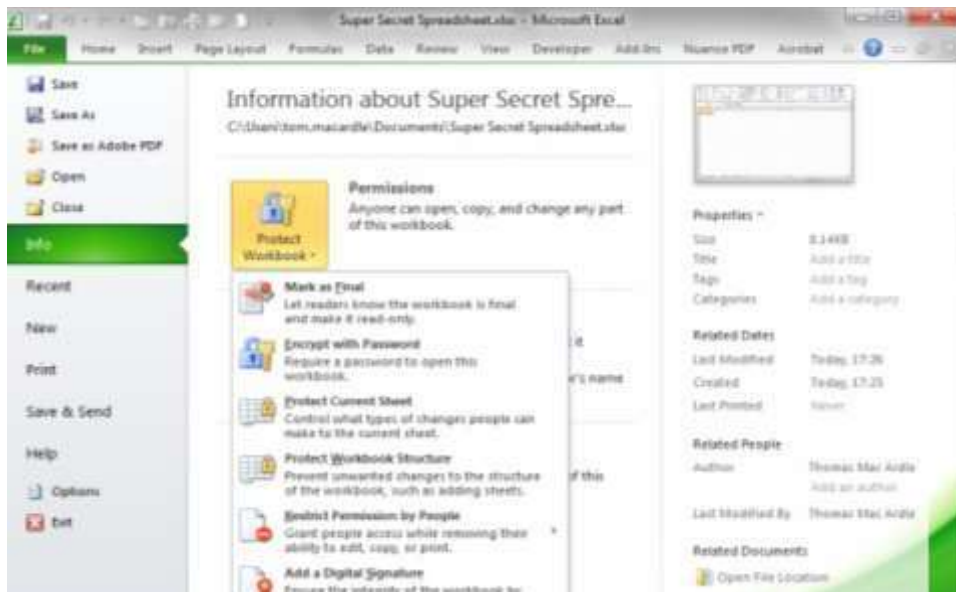
If you are sending documents to an outside source then phone the recipient with the password, don't e-mail it under any circumstances!! The password can be re-used but should be limited to one project to avoid it becoming well known.

Note: if you select any of the other options from the protect document dialogue box **the document will not be encrypted.**

*Respect Service Collaboration Excellence Justice Creativity*

## How to Encrypt an Excel Document:

Open the document you want to encrypt. Go to File, and select Info and select protect document. From the drop-down menu select Encrypt with Password.



Next dialogue box to open is the password box. Note you should enter a strong password – it should contain capital letter/s, lowercase letter/s, number and a symbol such as !+#!%. Remember once this is entered you or anyone else will not be able to access the document without the password. Create a separate word document to record the password, date, recipient and password used and store it in your home folder (O:/ drive).

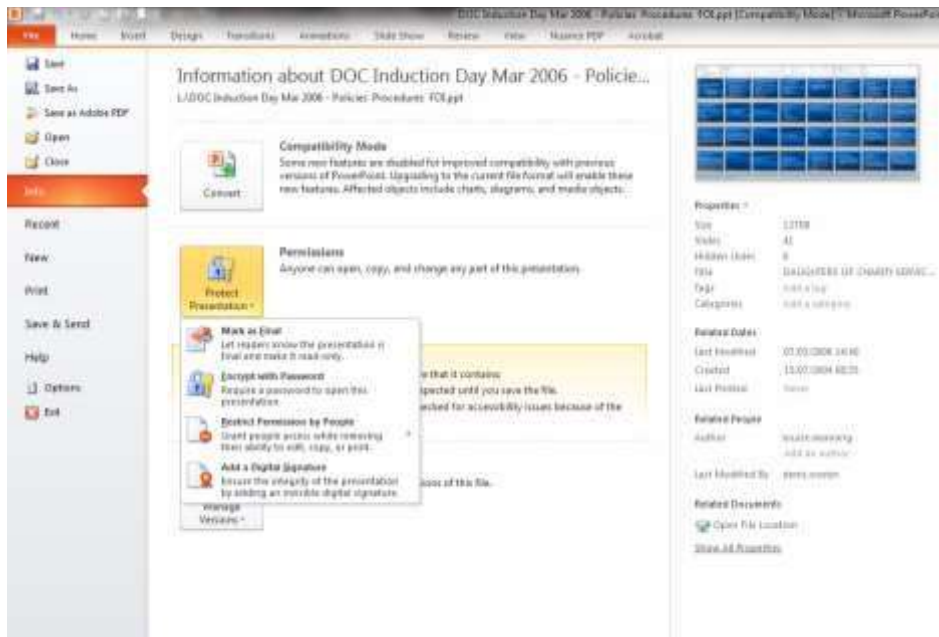


If you are sending documents to an outside source then phone the recipient with the password, don't e-mail it under any circumstances!! The password can be re-used but should be limited to one project to avoid it becoming well known.

Note: if you select any of the other options from the protect document dialogue box **the document will not be encrypted.**

## How to Encrypt a PowerPoint Document:

Open the document you want to encrypt. Go to File, and select Info and select protect document. From the drop-down menu select Encrypt with Password.



Next dialogue box to open is the password box. Note you should enter a strong password – it should contain capital letter/s, lowercase letter/s, number and a symbol such as !+##\*%. Remember once this is entered you or anyone else will not be able to access the document without the password. Create a separate word document to record the password, date, recipient and password used and store it in your home folder (O:/ drive):



If you are sending documents to an outside source then phone the recipient with the password, don't e-mail it under any circumstances!! The password can be re-used but should be limited to one project to avoid it becoming well known.

Note: if you select any of the other options from the protect document dialogue box **the document will not be encrypted.**

*Respect Service Collaboration Excellence Justice Creativity*

## **APPENDIX 4.2**      **Password guidance for picking strong passwords:**

Current advice from the National Cyber Security Centre in UK is to base passwords on *three random words* put together like 'coffeetrainfish' or 'walltinshirt'. The words need to be random words not related to each other – do not use your children's names!

You should use passwords based on who you deal with, one for Tusla another for HSE or the Limerick Avista etc. Too many passwords are bad for everyone and may lead to confusion.

### **Encryption Password Register**




Employee Name:

<b>File Name</b>	<b>Date</b>	<b>Sent To</b>	<b>Password</b>





## **APPENDIX 5**




## **Easy to Read Privacy Statement for a Data Breach:**



	<p>We must keep your information safe under Data Protection.</p>
	<p>If your information is misplaced, lost, stolen or disclosed to the incorrect person, you have a right to be informed.</p>
	<p>This is called a “Data Breach”.</p>
	<p>We will let you know what information about you has been misplaced.</p>

*Respect Service Collaboration Excellence Justice Creativity*

	<p>You have a right to ask questions about your information.</p>
	<p>We will support/reassure you and let you know what actions have been taken to locate your information.</p>
	<p>You have a right to ask questions on how we will keep your information safe and secure after this incident.</p>
	<p>If you are not happy about the data breach or the actions taken, you can make a complaint to the Data Protection Officer who will meet with you to discuss your concerns You can contact the Data Protection Officer at;</p> <p style="text-align: right;">Name: Marie Grimes McGrath  <a href="mailto:mgrimesmcgrath@lim-docservice.ie">mgrimesmcgrath@lim-docservice.ie</a>  Phone: 086-8189201</p>

	
 	<p>Your information- we are all accountable for your privacy.</p>