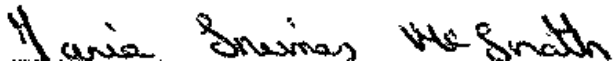
Legitimate Interests Policy & Procedure

Revision: **A**	**Department:** **Governance, Strategy and Planning**	**No:** **DOCS 087**
Prepared by:	 **Ms Marie Grimes McGrath** **Data Protection Officer**	**Date: 31/8/2021**
Approved by:	 **Ms Natalya Jackson** **Chief Executive Officer (CEO)**	**Date: 31/8/2021**

Review History

No	Old revision status	New Revision Status	Comment	Date	Prepared By	Approved by
1		A	Initial Issue	19/7/21	Marie Grimes McGrath, Data Protection Officer	Natalya Jackson, CEO

TABLE OF CONTENTS **Page**

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 employees, 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.

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.

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).* The Legitimate Interests Policy and Procedure 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.
- 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 Data 085 Data Protection Policy and Procedures.
- Avista DOCS 085, Data/Joint Data Controller and Third-Party Processor Agreement Templates (Appendices to this Policy).

4.0 ROLES AND RESPONSIBILITIES:

It is important that the organisation has a strong framework in place in relation to delivering on its commitment in meeting its obligations under the Data Protection Act 2018 and GDPR Regulations May 2018.

4.1 Board of Directors:

The Board of Avista is ultimately responsible for ensuring that effective internal GDPR Governance systems and processes are in place to enable compliance with Data Protection Legislation 2018, regulations and guidelines.

4.2 Chief Executive Officer:

The Chief Executive Officer has overall responsibility for ensuring that the organisation is upholding its legal responsibility to comply with the Data Protection Legislation.

4.3 Director of Governance, Strategy and Planning:

The Director of Governance, Strategy and Planning will be directly responsible for Data Protection on the Executive Team. Working with the Data Protection Officer (DPO), the Director of Governance, Strategy and Planning oversees policy and practice that seeks to ensure that the organisation meets all requirements as set out in the GDPR May 2018.

4.4 Data Protection Officer:

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

The Data Protection Officer is responsible for:

- In consultation with Senior Management and all stakeholders of the organisation, 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 the GDPR Regulations May 2018.
- Seeks to ensure that the rights of individuals with regard to the processing of personal information through data management practices are upheld. This will be monitored through the implementation of this Policy, where legitimate interests is relied on for the lawful purpose for the processing of personal information.
- Ensures that personal and non-personal information is only processed where the organisation has verified and met the lawfulness of processing requirements.
- Ensures that all employees are competent and knowledgeable about their Data Protection obligations, and are provided with in-depth training on the GDPR May 2018, to include the implementation of the Legitimate Interests Assessment (LIA), specific to their role and responsibility within the organisation.
- All Legitimate Interest Assessments (LIA) will be processed by the DPO in collaboration with the relevant departments. The DPO and the relevant department will retain a copy of all assessments completed.
- Maintains a continuous programme of monitoring, review and compliance with the GDPR May 2018 and to identify gaps and non-compliance before they become a risk, effecting mitigating actions, where necessary, to maintain compliance.
- 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.

Phone: 086-8189201 / 0505-22046 Ext 297

Email: mgrimesmcgrath@lim-docservice.ie

4.5 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 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.

5.0 KEY PRINCIPLES AND COMPONENTS:

5.1 GENERAL DATA PROTECTION REGULATION (GDPR):

The ***General Data Protection Regulation (GDPR) (EU) 2016/679***, hereafter referred to as ***the GDPR May 2018*** 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 State 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. Avista is the Data Controller for the personal and special categories of data processed in line with the definition of a Data Controller in Data Protection Legislation.

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).

5.1.1 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."*

5.1.2 Information Protected under the 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.

5.2 LEGITIMATE INTEREST UNDER DATA PROTECTION LEGISLATION:

The *General Data Protection Regulation (EU) 2016/679 (GDPR)* defines six legal bases under which personal data can be processed. Article 6(1)(f) defines legitimate interests as a lawful basis for processing where: -

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child."

A controller's ***interests*** can be defined as an advantage or benefit to them; or a stake in the processing or outcome. It is because of these ***'interests'*** that the Regulation warrants an evaluation when using this legal basis, with Recital 47 stating *"the existence of a legitimate interest would need careful assessment".*

5.3 RELYING ON LEGITIMATE INTERESTS:

Relying on legitimate interests as the grounds for processing personal data is only lawful when such processing is ***necessary,*** and any controller interests are ***not outweighed*** by the rights and freedoms of the individual. The GDPR also notes that legitimate interests cannot be relied upon by public authorities in the performance of their tasks.

The GDPR mandates the documenting of any Legitimate Interests Assessment and decision; as well as recording in the privacy notice any legitimate interests pursued by the controller or by a third party where processing is based on point (f) of Article 6(1).

5.4 ASSESSMENT STAGES:

Whilst the GDPR May 2018 does not specify the format for the Legitimate Interests Assessment, the UK Information Commissioners Office (ICO) and Article 29 Working Party (WP29) both refer to stages of the assessment for determining if legitimate interests are the most appropriate basis for processing.

The WP29's Guidelines on Transparency advise that: -

"The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the data controller should also provide the data subject with the information from the balancing test, which should have been carried out by the data controller to allow reliance on Article 6.1(f) as a lawful basis for processing".

The ICO have defined a 3-part test for assessing the use of legitimate interests and break those parts down into: -

1. Purpose.
2. Necessity .
3. Balancing .

5.4.1 Purpose:

Documenting the purpose of the processing and what function it serves for the controller provides the basis for identifying any legitimate interests and documenting them. Defining the purpose allows the controller to establish which legal basis is most appropriate and to move on to the other assessment stages if legitimate interests is deemed appropriate.

At this stage, all identified interests should be recorded; even if they are not all being relied on for processing. The questions set out in Part 3 Balance Test of the Legitimate Interests Assessment of this document help to produce responses that define the purpose and interests. The interests can be that of the controller or the interests of third parties, and commercial interests, as well as wider societal benefits. Interests that are persuasive and significant will be less easily overridden by an individual's rights and freedoms when carrying out the balancing test.

5.4.2 Necessity:

The ICO define *'necessary'* as ***"processing must be a targeted and proportionate way of achieving your purpose."*** You must be able to demonstrate that processing is necessary and evidence that there is no less intrusive way to achieve the same result. Consider the

organisation's interests noted from stage one and any business objectives relevant to the processing. Is the processing *'necessary'* to achieve those interests and objectives?

If you can identify another (*less intrusive*) way to achieve the same objective or interest (*or determine that the processing is not necessary*), then you should **not** be relying on Legitimate Interests.

5.4.3 Balancing:

The final stage of a Legitimate Interests Assessment (LIA) is to balance the processing against the individual's interests, rights and freedoms. This means documenting and demonstrating an evaluation of those rights and freedoms and ensuring that the individual's interests do not override that of the controller. This stage is about considering the impact the intended processing would/will have on an individual and evaluating any impact against the controller's identified interests.

5.5 LEGITIMATE INTERESTS ASSESSMENT (LIA):

The below Legitimate Interests Assessment (LIA) template can be used to determine if legitimate interests are the most appropriate legal basis for your processing. The questions in the assessment are not exhaustive; so, you should use your expertise, business knowledge and own judgement to make an informed decision. You should also customise the template and questions as to suit your processing activity and business type.

You should complete an assessment for each processing activity where legitimate interests are being relied on for the processing of personal data and ensure that this is reviewed periodically. These assessments commence on implementation of the policy across the organisation. This will include where there are any changes to the interests, purpose of processing, or any factors that could change the outcome of the assessment. An LIA should be completed in compliance with the Data Protection principles, the accountability principle and the GDPR May 2018 requirements.

1. PURPOSE TEST:		
Identify the purpose of the processing and the legitimate interests you intend to rely on:		
Ref:	**Assessment Question:**	**Response:**
1.1	What are you trying to achieve with the processing?	
1.2	What is the purpose of the processing?	
1.3	Who benefits from the processing*? (i.e. wider social interests, controller, third-party etc.)*	
1.4	Have you identified the relevant legitimate interests? ***If yes, what are they?***	
1.5	Are the noted interests identified as specific legitimate interests under the GDPR, Data Protection Bill or any other legislation or regulation?	
2. NECESSITY TEST:		
Determine if the processing is necessary and if any other, less intrusive option is available:		
Ref:	**Assessment Question:**	**Response:**

2.1	Can the interests/objectives be achieved in any other *(less intrusive)* way?	
2.2	Why is the processing necessary to achieve your interests/objectives?	
2.3	Is legitimate interests a targeted and proportionate way of achieving your purpose?	

3. BALANCE TEST:

Assess your interests against those of the individual and document any safeguarding measures:

Ref:	Assessment Question:	Response:
3.1	Do you have any relationship with the individual(s)?	
3.2	Would people expect you to use their data in this way?	
3.3	Does the processing have a minimal privacy impact on the individual(s)? ***If no, utilise the safeguards measures section in the outcome form.***	
3.4	How does the processing benefit the individual?	
3.5	Can you easily and legibly explain your reasons and interests in a Privacy Notice?	
3.6	Are you processing high-risk, special category or confidential information?	
3.7	Are you processing children's data?	
3.8	Is any individual likely to find the processing intrusive or raise objections?	
3.9	Is the processing likely to cause any distress or unwarranted harm?	
3.10	Do the rights and freedoms of the individual override your interests?	
3.11	Where using legitimate interests for direct marketing, is the individual given the opportunity to opt-out during the initial data collection and via simple, easy to access methods thereafter?	

LEGITIMATE INTERESTS ASSESSMENT DECISION AND OUTCOME:			
REFERENCE NUMBER:			***DIRECTIONS:*** *1. Complete each section and use the stage 1-3 answers to inform your decision. This is done in collaboration with the DPO.* *2. Be as detailed as possible so that clear evidence can be seen about your decisions and the assessment outcome.* *3. A Reference Number to each LIA will be assigned by the DPO and a record of these will be retained on the organisation's Register of Processing Activities (RoPA). The relevant Department and the DPO will retain a copy of each assessment when completed.*
ASSESSMENT LEAD:			
DATE:			
CONTACT DETAILS:			

1. ASSESSMENT BRIEF		
1.1	**SUMMARY:** *Give an outline of the reasons for completing the assessment and why legitimate interests are being considered.*	
1.2	**OBJECTIVES/INTERESTS:** - *What is the purpose of the processing and what interests have been identified?* *If relying on third-party or wider public interests, document what these are.*	
1.3	**POTENTIAL RISKS/IMPACT:** - *What risks does the processing pose and will there be any impact on the individual(s)?*	
1.4	**SAFEGUARDS:** - *Where there is any risk involved in processing or there is deemed to be an impact to any individual, it is important to put safeguarding measures into place to mitigate (where possible) the impact. These may have been identified during this LIA or could come from a risk assessment or associated Data Protection Impact Assessment (DPIA).* ***Such measures can include (but are not limited to): -*** *Encryption, pseudonymisation, data minimisation, restricted access, passwords, authentication protocols and other technical and organisational measures.*	

1.5	**BENEFITS:** - *Detail any benefits of the processing to the individual.*	
1.6	**SUBJECT RIGHTS:** - *Is the individual able to exercise their data subject rights (where applicable) through this type of processing. If your legitimate interests are compelling enough to override the individual's rights, state why.*	
1.7	**PRIVACY NOTICE:** - *What statement will you add to your Privacy Notice(s) to explain the use of legitimate interests for this processing activity?*	

2. OUTCOME AND DECISION:

After completing the 3-stage test and the above brief, you should now be able to decide if using legitimate interests is the most appropriate legal basis for your processing activity. If undecided, it is unlikely that this is the most appropriate basis.

Please explain in summary format why you are able to, or not able to, rely on legitimate interests for your legal basis: -

We <u>are</u> relying on legitimate interests for this processing activity: ☐	**We <u>are not</u> relying on legitimate interests for this processing activity: ☐**
Signed by:	**Print Name:**
Role:	**Department:**
Authorised by (DPO):	**Review Date:**

6.0 MONITORING, AUDIT AND REVIEW:

- The DPO will have overall responsibility for ensuring the appropriate governance systems are in place on all data management practices to include the implementation of the Legitimate Interests Assessment where applicable for the processing of personal information.
- The DPO will retain copies of all Legitimate Interests Assessments and shall be available to the Office of the Data Commissioner on request.

The Legitimate Interest Policy Avista DOCS 087 will be reviewed in accordance with changes to legislation, regulations and recitals from the European Commission.

7.0 LEGISLATION AND RELATED POLICIES:

- Data Protection Acts 2003, 1988, 2018.
- The General Data Protection Regulation May 2018.
- European Data Protection Commission Guidelines.
- Data Protection Policy and Procedures Avista DOCS 085.