

Data Protection Impact Assessment – Stage Two

What is it you're planning to do?

Explain the problem, need, issue or deficiency your project will address, and what kind of data processing it will involve. You may wish to include project plans or flowcharts.

Consider:

- What do you want to achieve?
- What is the intended effect on individuals?
- What are the benefits of the processing for your service, and the organisation more broadly?

See the main report

The Council will be involved in a pilot to issue, through Abundance Investments, a bond for retail investors including local residents. The purpose is to raise finance more cheaply than through existing arrangements and to improve engagement with residents.

The impact on those individuals who subscribe to the bond is to provide a comparatively 'safe' investment compared to other investments.

Benefits are highlighted further in the report

Describe the nature of the processing.

Consider:

- How will you collect, use, store and delete data?
- What is the source of the data?
- Will you be sharing data with anyone?
- What types of processing identified as likely high risk are involved?

You might find it useful to refer to a flow diagram or another way of describing data flows.

1. How will you collect, use, store and delete data?

Please see Data Protection Policy. They principally collect data directly from customers through the Abundance's online platform, with data stored in their cloud database.

2. What is the source of the data?

Please see Data Protection Policy. Customers provide data directly through the online Abundance platform and the actions they take on their platform.

3. Will you be sharing data with anyone?

Please see Data Protection Policy and their Privacy Policy. They only share customer data with certain service providers they use which are required to deliver the service they offer customers. For example, this includes service providers who they use for identity verification, email marketing, ISA providers and payment processing.

4. What types of processing identified as likely high risk are involved?

They do not consider they undertake any processing identified as high risk.

Describe the scope of the processing.

Consider:

- What is the nature of the data, and does it include sensitive “special category” or criminal offence data?
- How much data will you be collecting and using? How often? How long will you keep it? Have you reviewed/arranged an entry in the corporate records retention schedule?
- How many individuals are affected?

Abundance do not collect any special category or criminal offence data on customers.

The data they collect is related to who they are and their contact information (e.g. name, address, DOB, email, phone number) as well as information required to provide the Abundance service (e.g. bank account details, national insurance number).

Abundance collect data on each customer who opens an Abundance account and makes investments on their platform – that is currently about 7,000 people. As a regulated investment platform and ISA provider, they are required to retain data for up to 5 years (FCA regulations) or up to 6 years (HMRC).

Abundance have approximately 13,000 signed up customers and 7,000 investors.

Describe the context of the processing.

Consider:

- How much control will people have over their data?
- Would they expect you to use their data in this way?
- Do they include children or other vulnerable groups?
- Are there prior concerns over this type of processing or security flaws?
- Is it novel in any way?
- What is the current state of technology in this area?
- Are there any current issues of public concern that you should factor in?
- Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Yes – all customers have specifically signed up for Abundance's service and agreed to their Privacy Policy.

As an investment platform, all customers must be aged 18 or over. We do not provide a service to children or other vulnerable groups.

No, Abundance are not conducting any data processing which would be considered high risk or have any prior concerns and they do not see use of data as novel.

The technology they use is not innovative and is well understood by Abundance.

Abundance are not conducting any data processing which would be considered high risk or have any prior concerns.

Abundance are not signed up to a code of conduct or certification scheme. However, their regulation as an authorised FCA firm requires them to define a risk appetite and monitor residual risk related to data security which they do on a monthly basis at Board level through ir Risk Register. They set out that they also follow FCA guidelines on data ownership, classification and encryption, device and access management, security awareness, disaster recovery and incident response, and where possible align their practices to external frameworks and principles.

Do you intend to consult with affected stakeholders? If not why not?

Consider/explain:

- When and how you will seek individuals' views – or justify why it's not appropriate to do so.
- Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The Information Security officer has been consulted and is content with the information and is awaiting an external review of Abundance for further assurance.

Not planning on consulting with Stakeholders as the policies from Abundance are clear on what individuals are signing up to as part of the platform and there is no compulsion for any individual to have to invest through the community bond.

Describe compliance and proportionality measures.

Consider:

- What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome?
- How will you prevent function creep (using the data for more than the original purpose)?
- What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

This is included in their Data protection policy and privacy policy

They set out that they conduct a review of any new data they collect or any new form of data processing they conduct to ensure it falls within their existing data map, Data Protection Policy and Privacy Policy or, if it does not, to update their controls and inform customers if there is a change to their Privacy Policy.

Risk Assessment

Identify, list and classify risks.

#	Include associated compliance and corporate risks as necessary <i>The Data Protection Principles are reproduced in Appendix A – you may wish to refer to these when identifying risks</i>	Likelihood of harm	Severity of harm	Overall risk
		Remote, possible or probable	Minimal, significant or severe	Low, medium or high
1	Inappropriate release of personal data	Remote	Significant	Low
2				
3				
4				
5				

Risk Mitigation		
Risk #	Options to reduce or eliminate risk (Possible or Probable Risks only)	Effect on risk
1	Data privacy policy is clear on what Abundance are doing with personal information and where this is going	Accepted

Approvals

This assessment must be approved before the project proceeds to implementation stage.

	Signed	Date
Data Protection Officer		
DPO advice/actions:		
Head of Service <i>Signature by Head of Service indicates acceptance of DPO advice unless expressly overruled with reasons</i>		
This DPIA and completion of actions arising from it will be the responsibility of (insert name of responsible officer in service)		

Once approved, this document should be sent to dp@westberks.gov.uk

END

Appendix A

The Data Protection Principles (from the General Data Protection Regulations)

1. Personal data shall be:
 1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
 2. collected for specified, explicit and legitimate purposes and not further processed 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 ('purpose limitation');
 3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
 5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
 6. 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').