Atlantic Vantage Point

PRIVACY POLICY

Bringing perspectives and investing in tech
from both sides of the Atlantic.

Atlantic Vantage Point

Table of Contents

Atlantic Vantage Point

1. Applicability of this policy

The Privacy Policy applies to AVP as a whole.

As such, AVP must ensure that all of its employees, as well as all third parties processing Personal Data on its behalf, are duly aware of this Privacy Policy.

2. Compliance with applicable legislation

AVP undertakes to process Personal Data in accordance with the applicable legal framework and, in particular, the GDPR and the “Loi Informatique et Libertés”.

3. Objectives and scope of the Privacy Policy

This Policy sets out the minimum standards and requirements that AVP must comply with when processing Personal Data, either directly or through a third party.

Adjustments or adaptations may be considered for specific cases, in consultation with AVP's Data Protection Officer with the prior approval of the CEO.

4. Minimum standards and requirements applicable within AVP

4.1. Main principles

This Privacy Policy incorporates the core principles of the GDPR and is designed to ensure/demonstrate AVP’s compliance with the applicable legal framework.

- Personal Data must be collected in a lawful, fair and transparent manner in relation to the Data Subject; in principle, processing is lawful if one of the following conditions is met:
  - The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes,
  - Processing is necessary for the performance of a contract to which the Data Subject is - or will be - a party,
  - Processing is necessary for compliance with a legal obligation to which the Data Controller is subject,
  - Processing is necessary in order to protect the vital interests of the Data Subject or another natural person,
  - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller,
  - Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or a Third Party - except where such interests are overridden by the interests of the fundamental rights and freedoms of the Data Subjects.

- The processing of Sensitive Data can only be carried out if there is a valid legal basis, as identified by the GDPR and the Loi Informatique et Libertés.

- Personal Data must be collected for specified, explicit and legitimate purposes and are not further processed in a manner that is incompatible with those purposes.

- Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Personal Data must be accurate and, where necessary, kept up to date: Personal Data that are inaccurate having regard to the purposes for which they are processed shall be erased or rectified without delay.

- Personal Data must be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.

- Personal Data shall be processed in a manner that ensures appropriate security to the risk, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

- AVP must be transparent with the Data Subjects whose Personal Data are processed, in particular by informing them of the processing and providing them with details on how to exercise their rights.

- AVP must complete and keep up to date the record of Personal Data processing activities it carries out as Data Controller. This record must contain at least the following information:
    - The name and contact details of AVP and, if applicable, of its Data Protection Officer; o The purposes of the processing; o A description of the categories of Data Subjects; o A description of the categories of Personal Data;
    - The categories of recipients to whom the Personal Data have been or will be disclosed, including recipients in third countries or international organisations;
    - Where applicable, transfers of Personal Data to third countries or international organisations, and the identification of such third countries or organisations;
    - The time limits for erasure of the different categories of Personal Data;
    - A general description of the technical and organisational measures implemented to ensure the protection of Personal Data.

- Where AVP acts as a Data Processor, it must also complete and maintain a record containing the following information:
    - The name and contact details of AVP and of each Data Controller on behalf of which the AVP is acting and, where applicable, the name and contact details of the Data Protection Officer;
    - The categories of processing activities carried out on behalf of each Data Controller, o Where applicable, transfers of Personal Data to a third country or international organisation, including the identification of the said country or international organisation and documentation of the existence of appropriate safeguards;
    - A general description of the technical and organisational measures implemented to protect Personal Data.

- The procedures implemented will ensure a rapid response to requests from Data Subjects concerning the processing of their Personal Data.

- Where processing is to be carried out on behalf of a Data Controller, the Data Controller shall only use Data Processors providing sufficient guarantees in such a manner that the processing of Personal Data will meet the requirements of the applicable legal framework and this Policy.

Any processing activity subcontracted by the Data Processor to further Data Processors must be subject to a written agreement containing specific obligations.

- Data protection must be taken into account by design and by default. In particular, Personal Data must be minimised, pseudonymised or made anonymous by appropriate technical and organisational measures, to the extent possible, in order to ensure the application of the provisions on privacy by design.

- Data protection impact assessments must be undertaken for all relevant processing projects and prior consultation with the CNIL must take place for projects for which it is estimated that the risks would be high in the absence of mitigation measures.

- AVP must implement processes and controls to ensure that the Personal Data it processes is not sold to third parties outside the AXA Group, as the AXA Group has publicly committed.

4.2. Signature of the *Binding Corporate Rules* (BCR)

AVP must implement the AXA Group's Binding Corporate Rules (BCR), i.e. achieve the level of compliance required by the AXA Group's Binding Corporate Rules and adhere to them by becoming a party.

4.3. Communication, awareness-raising and training

This Privacy Policy and any guidelines provided should be appropriately communicated within AVP and made available on a file accessible to all employees.

AVP's Data Protection Officer ensures the follow-up of mandatory awareness and training sessions (e-learning or physical presence) by staff involved in Personal Data processing activities.

In addition, the AVP Data Protection Officer provides advice/information and ensures compliance with regulations relating to the protection of Personal Data within the entity.

4.4. Implementation of a process to ensure accountability

AVP implements compliance procedures to ensure compliance with its various safety, monitoring and liability obligations.

4.5. Control and monitoring

AVP is required to conduct an annual gap analysis of compliance with the principles set out in the Privacy Policy.

The Group DPO provides AVP's Data Protection Officer with a gap analysis tool (*annual self-assessment questionnaire*). These present the results of the annual self-assessment.

4.6. Incidents notification

A security incident is a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data.

AVP must implement an incident notification procedure to ensure that each incident is properly managed. In the event of a security incident, any person who discovers the incident should immediately inform AVP's Data Protection Officers.

When acting as Data Controller, any incident likely to result in a risk to the rights and freedoms of Data Subjects must in principle be notified by AVP to the CNIL within 72 hours and possibly to the Data Subjects.

5. Governance Personal Data within AVP

AVP legal representatives are responsible for compliance with the applicable legal, regulatory and contractual provisions. They also guarantee that AVP implements policies and processes that comply with this Privacy Policy.

The Data Protection Officer may, as required, request the assistance of an external consultant on GDPR issues.

This person is the key interlocutor in matters of Personal Data protection. They ensure dialogue with the operational units and enable data protection measures to be adapted to the operational realities of the company's activities.

The tasks of the Data Protection Officer within AVP consist, *a minima*, of :

- Advising and informing the Data Controllers, Data Processors and employees who carry out the processing of Personal Data about the obligations provided for by the applicable regulations on the protection of Personal Data;
- Monitoring compliance with these regulations and AVP policies, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, as well as related audits;
- Providing advice as regards the data protection impact assessment and monitoring its performance;
- Cooperating with the Commission Nationale de l'Informatique et des Libertés (CNIL) and acting as its contact point on issues relating to processing or any other issue;
- Responding to requests from Data Subjects concerning the processing of their Personal Data.

6. Entry into force – Modifications

In accordance with the provisions of the French Labour Code, this **Privacy Policy** is submitted to the AVP Executive Committee for approval on 01/11/2020 and is available for AVP employees in the AVP Dropbox.

The **Privacy Policy** will be reviewed periodically and whenever required by legal or regulatory changes.

Atlantic Vantage Point

7. Glossary

Article 4 of the GDPR provides the following information:

- **Data Controller:** the natural or legal person, public authority, agency or other body which, alone or jointly with others (**joint controllers**) determines the purposes and means of the processing of **Personal Data**.

- **Data Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

- **Data Subject:** the natural person who can be identified directly or indirectly with Personal Data.

- **Personal Data:** any information relating to an identified or identifiable natural person ("Data subject").

- **Sensitive Data : 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.

- **Processing :** 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.

- **Recipient:** 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 those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

- **Third party:** a natural or legal person, public authority, agency or body other than the data subject, **Data Controller, Data Processor** and persons who, under the direct authority of the controller or processor, are authorised to process **Personal Data.**

- **GDPR:** general data protection regulation (EU) 2016/679 of 27 April 2016.

- **Loi Informatique et Libertés :** Law n°78-17 of 6 january 1978 as amended.