Personal Data Protection policy

Reference Policies Manual: # 14	
Creation: 25/05/2018 (v.1)	Updates: 23/09/2019 (v.2) 04/05/2023 (v.3) 03/09/2024 (v.4)
Policy manager: DPO (Data Protection Officer)	
Responsible for the validation of the policy: Executive Board	

Update

Updates to this policy are initiated by the Executive Board and/or the Data Protection Officer (DPO).

All updates must be validated by the DPO.

In the event of an update, a new version of the policy is issued.

Update table:

Nature of the update	Update
Annual review of the policy with updates mainly linked to: - Implementation of recommendations after periodic control performed in 2023	03/09/2024

GDPR policy

The European Union adopted Regulation 2016/679 (the "General Data Protection Regulation" or "GDPR") which is applicable from 25 May 2018. The GDPR supervises the processing of personal data on European Union territory.

The General Data Protection Regulation covers data protection and privacy for all individuals in the EU. With a primary aim of transferring the control of personal data back to individuals, a unified regulation also means a simplified regulatory environment for international businesses. The GDPR also addresses the export of personal data beyond the EU and impacts doing business within Europe and worldwide. It is the largest change to data protection legislation in the last 20 years, and regulators have unprecedented power to impose fines and will require widescale privacy changes across every organisation.

However, it also represents a major opportunity to:

- transform our approach to privacy,
- harness the value of our data, and
- ensure our organisation is fit for the digital economy

Argos Wityu and GDPR

At Argos Wityu, we believe this new approach represents a significant step forward in the empowerment of individual privacy rights. This regulatory shift in the collection and processing of personal data will undoubtedly set the bar for data security, across the world. We are strongly committed to implementing the GDPR, both for our clients and within Argos Wityu.

The present data policy applies from May 25th 2018, onwards to the personal data collected by Argos Wityu Partners SA, 1B, Rue Jean Piret L-2350 Luxembourg and its subsidiaries, whether for their own purpose or for the benefit of the investment funds or holding companies they manage or advise. Argos Wityu processes personal data during its activities. The group has several offices, established in the territory of the European Union and in Switzerland. Its activity mainly targets European residents. This policy applies to the Group.

Definitions

Personal data

"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. (art. 4 GDPR Regulation)

An 'identifiable natural person' is deemed to be a natural person who can be who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location, data online identifier, or to one or more factors specific to his or her physical elements specific to its physical, physiological, genetic, mental, economic, cultural or social identity, genetic, psychological, economic, cultural or social identity'.

The identification of a natural person can be carried out:

- from a single piece of data (e.g., social security number, DNA);
- revealing the alleged racial or ethnic origin ;
- dealing with political, philosophical or religious opinions (ex: trade union membership);

- from genetic or biometric data;
- data on offences or criminal convictions
- from the crossing of a set of data (e.g., a woman living at a given address, born on a given day, subscribed to such a magazine and activist in such an association).

Personal data processing

A "processing of personal data" 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. The Group processes personal data as part of these activities. This concerns investors or potential investors, investment companies, suppliers, employees, managers, consultants, prospects, etc.

On the other hand, a file containing only company contact information (e.g., "Company A" with its postal address, the telephone number of its switchboard and a generic contact email "compagnieA@email.fr") is not processing personal data.

Processing of personal data is not necessarily computerized: paper files are also a concern and must be protected under the same conditions. Data processing must have a purpose: Argos cannot collect or process personal data simply because it could be helpful to us one day. There must always be legal and legitimate reasons behind personal data processing.

Personal data breach

Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Consent

This means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by an explicit affirmative action, signify agreement to the processing of personal data relating to them. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

Cookies

Cookies are "mini files" that can be placed on a device connected to the Internet, such as a computer, phone, tablet or smart TV. Cookies can collect or store information about how the data subject behaves on (a website) and on their device. For more information, please visit cookies policy section on the website.

What personal data do we process?

Argos is collecting and using the personal data required in the framework of business (including regulatory framework), to provide its business partners and counterparts a high quality of service or interaction. For that purpose, Argos might collect different categories of your personal data, including:

- identification data (name, birth data, picture, address and contact details, passport or ID numbers, etc…)

- data related to your business positions and activities (employers and their contact details, positions and curriculum, etc)

- data about Argos interactions (emails, meetings or calls, agreements with you on draft or executed form, notes, etc…)

- if you are an investor or business partner as an individual, all the documentation shared prior to your subscription: your banking details and all the financial transactions with you; data related to the proper execution of legal, tax or regulatory obligations (anti-money laundering regulations, fund management records, justification of your investor status if applicable, FATCA / CRS and other tax reportings, etc).

- data related to activities related to philanthropic, social or business association activities in which members of the Group are engaged.

Argos does not collect nor process any personal data regarding religion, ethnic or racial origins, political opinions, sexual life or genetic information.

As data controllers, Argos must ensure the use of personal data that respects the privacy of the data subjects.

Some of Your Personal Data may be collected automatically, including technical information, including anonymous data collected by the host server for statistical purposes, the IP (Internet Protocol) address used to connect your computer or device to the Internet, browser type and version, time zone setting, browser plug-in types and versions, operating system, and platform. Please refer to cookies policy available on Argos Wityu's website.

For what purposes do we collect and use personal data?

Argos collects and use your personal data to:

- comply with the legal or regulatory obligations;
- interact with you commercially or for the purpose of analysing or elaborating an agreement with you;
- if you are an investor or the representative of an investor, to interact with you in respect of that position (including for reporting purposes);
- if you are a potential candidate, to be able to check the adequacy of your profile with identified needs, and to contact you;
- serve Argos legitimate interests in the framework of the GDPR Directive, including to keep evidence of interactions or dealings, to manage databases and information systems, to back up such databases and systems, to prevent frauds or abuses, to compile anonymous statistics, to analyse and prepare transactions, etc;

To whom might we communicate your personal data?

Argos does not sell nor lease your personal information to third parties. Argos do not share your personal data with third parties unless:

- Argos has a legitimate reason for that (eg sharing with lawyers to prepare a contract with you, or with a bank to prepare a payment to you), or
- Argos has your explicit consent, or
- an applicable law or regulation requires the Group to do so.

Please note that in certain cases Argos Wityu may be required to transfer Personal Data outside the European Union to comply with FATCA regulation (Foreign Account Tax Compliance Act). In this context, Argos Wityu must provide sensitive and financial information regarding bank accounts possessed by American Taxpayers (regardless of their place of residence) to the US tax authorities.

Argos Wityu internal organisation

Appointment of a Data Protection Officer at the group level

Argos has appointed a DPO: Data Protection Officer.

A dedicated email address dpo@argos.fund is used to centralize communications on GDPR topics.

Documentation

Argos keeps a data processing register as recommended in Article 30 of the GDPR to meet regulatory obligations. The data processing register is a mapping of the processing of personal data, which consists of identifying and listing all the processes and treatments within the Group, allowing us to determine precisely:

- The stakeholders (representatives, subcontractors, co-managers, etc.) involved in data processing;
- The categories of the data processed;
- What is this data used for (what does Argos do with it, who access it, and to whom are they communicated);
- How long does Argos keep the data;
- How does Argos secure the data.

Contracts/Third parties

The Group ensures that its partners comply with the GDPR rules and provides the contractual provisions of its commitments. Each team member must check his interlocutors/service providers comply with GDPR legislation.

In addition, the GDPR requires that the relationship between the controller and the data processor be strictly regulated and formalized in a written contract. This contract must contain several mandatory terms and clauses, including a clause authorizing the controller to audit how the subcontractor processes the data on his behalf or a clause organizing the subcontractor's staff access to the data. An update on the contracts with subcontractors is recommended if they do not comply with these clauses. Relevant teams must pay particular attention to the terms and conditions of the contracts they use in the Group's mission context.

The Group does not usually transfer data outside the European Union. However, if such a transfer is considered, Argos must check whether the non-EU country in which the company is transferring the data has data protection legislation and whether it is recognized as adequate by the European

Commission. If not, the relevant teams must contact the compliance department and DPO before transferring.

Access protection

The IT policy enables Argos to best guarantee the security and integrity of data by minimizing the risk of data loss or hacking. Passwords protect user accounts. Argos' employees have received a copy of the computer procedure and are aware of computer security issues (e.g., GDPR guidelines). They are thus made aware of the internal rules for managing personal data and the basic rules of security (e.g., complex log-in and personal password, workstation locked as soon as one is not at their desk, not storing professional documents on individual tools, etc.). Restricted access is provided for some data types, such as human resources, taxation, credit card, etc. Access to the premises of our various offices is secured (badges, keys, codes).

Data Retention

Argos Wityu does not store your Personal Data longer than is required. Storage periods may vary according to the types of data and processing. Argos processes and uses your Personal Data in accordance with applicable data protection regulations and will retain your Personal Data as long as is required by operational, regulatory and legal constraints, mainly to meet the storage obligations for certain documents and according to the applicable limitation periods.

Teams must isolate personal data in separate folders. Argos has a procedure for backing up and recovering data in the event of an incident.

Argos stores the data for no longer than is necessary for the purposes for which it is processed.

Examples of data retention:

- Tax documents: 6 years after the due date or termination.

- Documents collected to comply with money laundering and terrorist financing regulation: 5 years after cessation of relations with the person concerned.

Exercise of rights

The GDPR reinforces the obligation of information and transparency regarding the people whose data Argos process (investors, managers, employees, etc.). Collecting and processing personal data primarily involves informing people about what Argos does with their data and respecting their rights

The GDPR REGULATION establishes a number of rights in your favour, including, within the limits of law and regulations:

- the right to access your personal data
- the right to have your personal data rectified if inaccurate
- the right to have your personal data deleted if no longer kept for legitimate purposes
- the right to oppose the use of your personal data for commercial prospection purposes
- the right to withdraw your consent.

Please note that some legal restrictions limit those rights, for instance as regards Argos ability not to disclose information used in the processes against fraud or money-laundering.

In accordance with general principles of law, Argos is not liable for the disclosure of information that was previously publicly available, nor for the storage and backup of data that we received without having solicited (eg CV spontaneously sent to us) To use those rights, or more generally for information, you can reach the Data Protection Officer on the following e-mail address: dpo@argos.fund

The people whose data is processed (employees, service providers, etc.) can exercise rights to their data: right of access, rectification, opposition, deletion, portability, and limitation of processing.

Argos provides the means to effectively exercise these rights by creating a single email box dpo@argos.fund which allows people to contact the DPO directly.

The DPO must follow up on requests within one month of receiving them.

Incidents management

If the Group has suffered a data breach, Argos must report it to the French data Protection Authority (Commission Nationale de l'Informatique et des Libertés – CNIL) within 72 hours if this violation is likely to represent a risk to the rights and freedom of the persons concerned. This notification is made online on the CNIL website.

To determine the level of risk related to the incident, Argos evaluates it according to the following:

- Personal data has been encrypted;
- If the data is encrypted, assess the level of encryption;
- To what extent the data has been pseudonymized;
- The data in question concerns name, address, bank details;
- The volume of data;
- The number of natural persons affected;
- The nature of the incident: intentional or accidental.

The incident must be communicated as soon as possible to the DPO and CIO, who will take care to inform the Managing Partners.

When an incident is proven, and the risk is high, Argos has set up an incident file so that it is communicated to the competent authorities (ex: CNIL) and to the people involved in the incident.

This incident report must be communicated following the consequences of the latter and the risks it represents vis-à-vis the rights and freedoms of the person concerned (GDPR Article 33). The form must include information such as:

- The category and number of the natural persons concerned,
- Their names, first names and personal information.
- A description of the consequences of the incident,
- Measures taken to mitigate its effects.

Finally, as Argos Wityu is a European Group, If the breach occurs in the context of cross-border processing, the data controller will need to notify the CNIL and the local DPA (Data Protection Authority) where the breach occurred.

How to notify the incident

Notify the supervisory authority

The following sections describe the approach necessary to notify the incident to the competent authority:

The name of the authority:

National Commission on Informatics and Liberty (CNIL)

The address: 3 Place Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07

The phone: 01 53 73 22 22

The process:

The DPO must use the breach notification service to notify the CNIL of a data breach.

The following information must be notified:

- The nature of the personal data breach, including insofar as possible,
- The surnames, forenames and personal information of the persons concerned.
- A description of the consequences of the incident
- Measures taken to mitigate its effects.

If the notification has been sent more than 72 hours after its discovery, Argos must justify the reasons for the delay.

Inform the persons concerned.

The GDPR requires Argos to inform all natural persons involved in an incident about the personal data that could impact their rights and freedom (GDPR Article 34). The risk associated with this incident must be high to justify the notifications of the parties concerned. If steps have been taken to mitigate the consequences of the incident and they do not bring the risk to a high level that may affect the rights and freedoms of the person, then notification is not necessary.

The notification must be given as soon as possible through the appropriate secure means to the organization; and it must contain the following information:

- Th nature of the data breach;
- A description of the likely consequences of the violation of personal data;
- A description of the measures taken or proposed to address the personal data breach, including when appropriate measures to mitigate its potential adverse effects;
- The name and contact details of the DPO where further information is to be submitted.

It will be appropriate to notify the concerned person of the nature of data affected by email to ensure that the messages have been received and that they can take all necessary measures.

Review of the policy

This policy will be regularly updated; Argos invites you to visit regularly our websites to be aware of the latest version of our GDPR policy and use your right to withdraw your consent if you do not agree with its terms.