GENERAL PERSONAL DATA PROTECTION POLICY

Preamble

Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, which came into effect on May 25, 2018, regarding the protection of natural persons concerning the processing of personal data and the free movement of such data (hereinafter "GDPR") states in its preamble that the protection of natural persons concerning the processing of personal data is a fundamental right.

Sfil and Caffil (hereinafter "the Sfil Group") are committed, in accordance with the applicable legislation, to ensuring the protection, confidentiality, and security of personal data collected and processed in the course of its activities, as well as to respecting privacy.

This policy aims to present, in a single document, clear, simple, and precise information regarding the processing of personal data implemented by the Sfil Group in its capacity as data controller. It is an integral part of the general terms and conditions of use of the Sfil / Caffil Group website.

This policy allows individuals from whom the Sfil Group collects and/or processes personal data in the course of its activities to understand how their personal data is used. The individuals concerned are those with whom the Sfil Group interacts: clients, prospects, partners, borrowers, job candidates, investors, suppliers, service providers, and other users of its services, including visitors to the Sfil / Caffil Group website.

1. Definitions

To ensure a good understanding of the key principles and rights outlined in this General Personal Data Protection Policy, it is necessary to first present the definitions of its main key terms.

1.1. Personal Data

Personal data refers to any information relating to an identified or identifiable natural person.

For example, personal data includes: name, surname, phone number, photograph, video recording, biometric data, social security number, postal address, email address, age, etc.

1.2. Sensitive Personal Data

Among personal data, there are specific categories of data commonly referred to as "sensitive data." These include data revealing, directly or indirectly, racial or ethnic origin, political, philosophical, or religious opinions, trade union membership, or related to health, sexual life, or sexual orientation, as well as genetic and biometric data.

In principle, the processing of such data is prohibited, except in strictly enumerated cases in Article 9 of the GDPR such as:

- The data subject has given explicit consent to the processing for one or more specific purposes,
- The processing is necessary for the performance of obligations and exercise of rights specific to the data controller or the data subject in the field of labor law, social security, and social protection,
- The processing relates to personal data that have been manifestly made public by the data subject,
- The processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts act in their judicial capacity,
- The processing is necessary for preventive medicine or occupational medicine, assessment of the worker's capacity, medical diagnosis, health or social care, or management of health care systems and services.

In addition to these specific categories of data governed by Article 9 of the GDPR, other data classified as "highly personal" due to their potential impact on an individual, such as data related to criminal convictions or security measures, social security number (NIR), or bank details, are also subject to special precautions during processing.

1.3. Data Subject

The data subject is the natural person to whom the personal data being processed relates.

Certain data subjects are classified as "vulnerable" due to the increased power imbalance that may exist between these individuals and the data controller. This includes minors, employees of a company, and individuals under legal protection. Specific measures are implemented to frame the processing when the data subjects are vulnerable.

1.4. Data Controller

The data controller is the person, entity, service, or other organization that determines the purposes and means of processing personal data.

1.5. Processor

Generally, a processor is any person, entity, or service processing personal data on behalf of the data controller. For example: a data hosting provider, an application maintenance provider.

1.6. Processing of Personal Data

Processing of personal data means any operation or set of operations performed on such data, regardless of the process used, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, communication by transmission, dissemination or any other form of provision, combination or interconnection, as well as the locking, erasure, or destruction of personal data. Processing of personal data is not necessarily automated; this policy also applies to processing implemented on paper-based records.

1.7. Recipient

The recipient is the natural or legal person, public authority, service, or other organization that receives communication of personal data, whether or not a third party.

2. Governance of Personal Data

Dedicated to protecting the privacy and personal data of its clients, prospects, partners, borrowers, job candidates, investors, suppliers, service providers, employees, and other users of its services, the Sfil Group has established appropriate governance to ensure the protection of personal data in compliance with the legal and regulatory requirements related to the use and protection of such personal data.

Furthermore, the Sfil Group has defined the following framework:

A Personal Data Protection Charter that specifies, among other things, all the guiding principles applicable to the collection and processing of personal data,

A Charter for the use of Generative Artificial Intelligence that governs user practices,

The DPO, appointed for the Sfil Group, is tasked with ensuring compliance with data protection regulations by the data controller and cooperating with the French data protection authority (CNIL) on matters related to personal data processing. He serves as the point of contact for the CNIL and all individuals concerned by the collection or processing of personal data.

2.1. Employee Awareness and Training

Employees are required to complete and validate at least one e-learning training module "Personal Data Awareness" at defined intervals.

2.2. Protection of Your Personal Data

The Sfil Group places particular importance on the security of personal data.

It implements technical and organizational measures appropriate to the sensitivity level of personal data to ensure the security, integrity, and confidentiality of the data and to protect them against any malicious intrusion, loss, alteration, destruction, misuse, or disclosure to unauthorized third parties. For example: application protection through strong authentication, access to secure premises, implementation of distinct profiles according to user data access needs, etc.

The security of personal data also relies on the compliance of Sfil Group employees with the Personal Data Protection Charter. This security is also contingent upon the adherence of our service providers to the security rules defined by the Sfil Group.

2.3. Regulation of Cross-Border Flows

Personal data processed by the Sfil Group in the course of its activities may be transferred to countries outside the European Economic Area (EEA).

When personal data is transferred to countries outside the EEA, these data may be subject to legislation or regulations that vary in their level of protection regarding personal data and may not always be recognized as equivalent to that offered by European Union law.

In the event of such a transfer to a non-EEA country, the Sfil Group will ensure that this transfer is governed in accordance with applicable European regulations, thereby ensuring the protection and security of personal data transferred outside the EEA. Specific and additional security measures may be implemented to ensure that these transfers comply with the requirements of the GDPR and the guidance of the relevant protection authorities.

2.4. Notification of Personal Data Breaches

A personal data breach is defined as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of personal data transmitted, stored, or otherwise processed, or unauthorized access to such data" (art.4 §12 of the GDPR).

In accordance with Article 33 of the GDPR, the Sfil Group, as the data controller, is obligated to document any personal data breach of which it becomes aware. The procedures in place provide for, if necessary, notification to the CNIL as soon as possible and no later than 72 hours after becoming aware of it. If a personal data breach presents a high risk to the rights and freedoms of the individuals concerned, the Sfil Group will inform them as soon as possible of the nature of the breach and all measures taken to remedy it.

To this end, the Sfil Group has an internal procedure that allows for compliance with this regulatory obligation and maintains a registry of data breaches in which breach incidents are recorded.

2.5. Internal Control System

The Sfil Group implements the necessary means to ensure compliance of its processing with data protection regulations.

The DPO ensures, in accordance with Article 39 of the GDPR, the monitoring of compliance with the GDPR, all regulations regarding the protection of personal data, as well as internal rules concerning personal data.

The Sfil Group has a **Framework Policy for Internal Control**, which refers to all systems aimed at managing activities and risks of all kinds, ensuring the regularity, security, and efficiency of operations. Like other risks faced by the Sfil Group, the GDPR compliance control system fits within this framework. The overall architecture of the Sfil Group's internal control system is based on **a risk map that includes a GDPR Compliance component**. The internal control system itself is based on three levels constituting the three lines of defense, ultimately under the responsibility of the Sfil Group's general management and supervised by the Sfil Group's board of directors, the Caffil management board, and its supervisory board.

The Sfil Group is also required to conduct periodic audits to ensure that its service providers comply with the security rules defined in the contracts that bind them to the Sfil Group.

3. Data Controller

The data controller of your personal data is the Sfil Group, a public limited company with a board of directors approved as a credit institution by the Prudential Control and Resolution Authority located at 112-114, avenue Emile Zola – 75015 Paris.

The Sfil Group has appointed a Data Protection Officer (DPO), registered with the CNIL.

To exercise your rights or for any questions regarding this General Personal Data Protection Policy, the Sfil Group's Data Protection Officer (DPO) can be contacted by any interested party via email at:

dpo@sfil.fr

or at the following postal address:

DPO Sfil
112-114, avenue Emile Zola
75015 Paris

4. Principles Applicable to Personal Data

The Sfil Group is committed to respecting the principles set forth in Regulation (EU) 2016/679 regarding the collection and use of personal data.

4.1. Legitimate and Proportional Use

Personal data is collected by the Sfil Group for specific, explicit, and legitimate purposes related to its activities. The collection of personal data within the Sfil Group is intended for the exercise of its activities in the context of its relationships with its employees, clients, prospects, partners, borrowers, job candidates, investors, suppliers, service providers, and other users of its services. For each processing activity, the Sfil Group commits to only collecting and processing data that is strictly necessary for the pursued objective.

4.2. Fair and Transparent Collection

In a spirit of fairness and transparency towards its clients, employees, partners, suppliers, service providers, investors, or any other individuals concerned whose data it processes, the Sfil Group ensures that individuals are clearly informed about each processing activity it implements through information notices displayed or indicated on various media: website, collection forms, information notices, etc. Personal data is collected fairly. No collection is made without the knowledge of the individuals concerned or without duly informing them.

4.3. Relevance and Minimization of Collected Data

The personal data collected are strictly necessary for the purpose pursued by the data collection. The Sfil Group strives to minimize the data collected, ensuring that it is accurate and up to date. The Sfil Group only collects and processes the personal data it needs to fulfill the purpose of processing.

4.4. Limitation of Data Retention Periods

The Sfil Group commits to ensuring that the retention periods applied to the data are proportionate to the purposes for which they were collected. To this end, the Sfil Group retains collected personal data only for the duration necessary concerning the purposes of the processing in question and in accordance with applicable national legislation, particularly concerning statutory or regulatory retention periods. *For example, in the context of anti-money laundering and counter-terrorism financing measures, data is retained for five (5) years from the end of the business relationship.*

4.5. Data Integrity and Confidentiality

Personal data is processed by the Sfil Group to ensure an appropriate level of security for this data, including protection against unauthorized processing of this data by third parties, loss, destruction, alteration of this data, or any incident that may render this data unavailable and may cause harm to the individuals concerned.

The measures taken aim to ensure the integrity of this data and to provide adequate confidentiality in relation to its nature and sensitivity, so as to limit any access by unauthorized third parties to this data.

4.6. Data Protection by Design and by Default

The Sfil Group implements measures designed to adhere to the principles of data protection by design and data protection by default.

Thus, when developing internally initiated projects or selecting and using applications, services, and products that rely on the processing of personal data, the Sfil Group inherently integrates all principles and rights related to data protection.

It ensures that software or digital solution publishers/providers meet legal requirements and ensure the protection of the data being processed.

5. Processing of Your Personal Data

5.1. Types of Personal Data Processed

The Sfil Group collects and processes several categories of personal data which may include:

• Identification data (name, surname, date and place of birth, nationality, photo, ID number, etc.);
• Professional or personal contact details (email and postal addresses, professional or personal phone numbers, etc.);
• Information collected as part of a recruitment process;
• Data from phone recordings, video surveillance (for example, security monitoring of our premises);
• Any other personal data that may be communicated to the Sfil Group.

Personal data may also be collected directly from you during our interactions (in-person or phone interviews in compliance with applicable rules), when you visit our websites by filling out a contact form, when you send us an email, when you apply for a job offer, etc.

They may also be collected indirectly through third parties (publications, service providers, suppliers, publicly accessible websites, databases, etc.).

5.2. Purposes: Specific and Legitimate Objectives for Which the Sfil Group Collects and Processes Your Personal Data

In accordance with the applicable regulations, in general, we use personal data to:

• Comply with our legal or regulatory obligations, including banking and financial regulations, anti-money laundering, and counter-terrorism financing;
• Conclude contracts;
• Manage an ongoing contract;
• Contact you regarding the signing of a contract, process tenders issued by the Sfil Group in which contact details of suppliers and potential service providers may be collected;
• Maintain relationships with our investors for whom contact details may be collected via the Sfil Group websites or by Sfil Group employees, to whom the Sfil Group may send financial communications or invitations to financial communication events;
• Pursue our legitimate interests, namely to manage our risks, ensure the protection of our rights by retaining proof of transactions;
• Manage recruitment processes;
• Respond to inquiries from investors or journalists;
• When the Sfil Group has collected your consent via the contact form on one of the Sfil Group websites: by subscribing to our alerts, you consent to receive by email information related to the Sfil Group. You can unsubscribe at any time by clicking the link provided in each of our communications;
• Respond to official requests from duly authorized public or judicial authorities.

Your personal data is not subject to any fully automated decision-making.

5.3. Legal Basis: Legal Foundations for the Processing Implemented by the Sfil Group

Every processing implemented by the Sfil Group is based on a legal foundation.

Thus, the processing activities carried out by the Sfil Group are only conducted if at least one of the following conditions is met:

i. Legal or Regulatory Obligations

Certain personal data processing activities carried out by the Sfil Group may be necessary to comply with legal or regulatory obligations imposed on the Sfil Group as the data controller. For example, legal or regulatory obligations related to anti-money laundering or counter-terrorism financing processing, or obligations related to declarations to social security agencies by the Sfil Group as an employer.

ii. Execution of the Contract or Pre-Contractual Measures with the Data Subject

Processing may also be implemented and is lawful when it is strictly necessary for the execution of a contract binding the Sfil Group with the data subject, or for the execution of pre-contractual measures taken at the request of the latter.

iii. Consent of the Data Subject

Certain personal data processing activities are carried out based on the consent of the data subject. In this case, the consent of the data subject constitutes the lawful basis for the processing.

For these processing activities, the Sfil Group ensures that consent is freely given, informed, unambiguous, and provided through a clear affirmative action, for example, through a written declaration, including electronically.

Similarly, the Sfil Group ensures that the data subject can withdraw their consent at any time and has been informed of this possibility prior to the collection of their consent.

iv. Legitimate Interests of the Sfil Group

The legitimate interests of the Sfil Group may also justify the processing of personal data.

In this case, the processing must take into account the interests and fundamental rights of the individuals concerned, which must be framed by specific measures and guarantees to ensure the protection of the interests and rights of individuals. The balancing of interests ensures that there is a balance between the legitimate interests pursued by the Sfil Group and those of the data subject.

5.4. Recipients of Personal Data

The personal data we collect is intended for us as the data controller.

The Sfil Group ensures that only authorized persons can access this data. Within the various departments of the Sfil Group, personal data is only accessible or transmitted to authorized individuals based on their missions.

To fulfill the purposes described in paragraph 5.2, the Sfil Group may, in certain cases, communicate personal data to the following external stakeholders:

- Service providers performing services on its behalf, including regulated professions (lawyers, notaries, auditors);

- Judicial or financial authorities, state agencies, or public bodies upon their request and within the limits permitted by the regulations.

Your personal data may also be subject to reconciliation, sharing, or pooling among all entities of the Sfil Group or its shareholders.

They may be communicated to these entities for the above-mentioned purposes in this Personal Data Protection Policy.

5.5. Processors

The Sfil Group carefully selects its processors and requires them to:
• Provide a level of personal data protection equivalent to that which it grants to this data,
• Use personal data only to manage the services they are required to provide,
• Strictly comply with applicable laws and regulations regarding confidentiality, banking secrecy, business secrecy, and the protection of personal data,
• Implement all adequate measures to ensure the protection of personal data they may process,
• Define the technical and organizational measures necessary to ensure the security of this data.

The Sfil Group commits to entering into contracts with its processors that specify the conditions and modalities of personal data processing carried out on its behalf, in accordance with Article 28 of the GDPR.

5.6. Retention Periods for Your Personal Data

Respectful of the right to be forgotten, the Sfil Group commits to ensuring that the retention periods of personal data are proportionate to the purposes for which they were collected. These periods are defined in accordance with applicable national legislation, particularly concerning statutory or regulatory retention periods.

For example, in the context of anti-money laundering and counter-terrorism financing, data is retained for five (5) years from the end of the business relationship with the Sfil Group.

5.7. Collected Cookies

We may process your personal data using "cookies" technology. Indeed, when you visit one of the Sfil Group's websites, it collects a "cookie," which is a small file stored on your device when you visit a site. The cookie records information about your device, your browser, and, in some cases, your preferences and browsing habits.

In a spirit of information and transparency, the Sfil Group has a Cookies Policy intended to inform website users about the origin and purpose of navigation information processed during their consultation of the sites, as well as their rights.

Our Cookies Policy is available on each of our Sites, in the "personal data" section.

6. Rights of Individuals: Rights Recognized to You

Individuals whose data is processed by the Sfil Group (clients, employees, service providers, etc.) have rights regarding their data and the processing carried out on it. The Sfil Group is committed to respecting these rights in accordance with applicable legislation and regulations, and in this context, it ensures the respect of the following rights:

• The right to be informed about processing,

• The right of access and rectification,

• The right to erasure or "right to be forgotten,"

• The right to limit processing,

• The right to data portability,

• The right to object to processing,

• The right to withdraw consent at any time,

• The right to lodge a complaint and seek redress.

6.1. The Right to Information about Processing

This General Personal Data Protection Policy informs you of the purposes, legal framework, interests, and recipients or categories of recipients with whom your personal data is shared.

In order to ensure fair and transparent processing, the individual whose data is processed by the Sfil Group receives clear and complete information regarding:

• The identity and contact details of the data controller, its legal representative, and its data protection officer (DPO), if applicable;
• The purposes of the processing as well as the legal basis for the processing;
• If applicable, the legitimate interests pursued by the data controller or a third party;
• In the case of indirect collection of data: the categories of personal data concerned;
• In the case of data collection directly from the individual: whether the provision of data is mandatory or optional, as well as the possible consequences of not providing the data;
• The recipients or categories of recipients to whom the personal data is communicated;
• If applicable, the existence of transfers of data to a third country outside the European Union or an international organization, the existence of an adequacy decision covering this transfer, or failing that, the appropriate safeguards implemented to govern this transfer and the possibility of obtaining a copy of them;
• When possible, the anticipated duration of retention of personal data or, when this is not possible, the criteria used to determine this duration;
• The existence of the right to request the data controller to access their personal data, rectify or erase them, limit processing, or port their data; the right to object to the processing of their data under certain conditions; the right not to be subject to a decision based solely on automated processing, including profiling; the right to define specific directives regarding the fate of their data after their death; when the processing is based on the consent of the individual; the right to withdraw their consent at any time; and the right to lodge a complaint with a supervisory authority;
• If the personal data is not collected from the data subject, any available information regarding its source;
• The existence of automated decision-making, including profiling, and, at least in such cases, useful information regarding the underlying logic, significance, and expected consequences of this processing for the data subject.

When the Sfil Group intends to carry out further processing of the personal data of the data subject for a purpose other than that for which their personal data was collected, the DPO ensures compliance with the requirement of compatibility of this new processing purpose with the initial purposes of processing and will provide the data subject with information regarding this new processing beforehand.

6.2. The Right of Access and Rectification of Your Data

You have the right to access and rectify your personal data, which you can exercise with the Sfil Group by providing proof of your identity at the following email address: dpo@sfil.fr.

In this regard, you can obtain information regarding the processing of your personal data.

At your request, we can rectify and/or complete your personal data if it proves to be inaccurate, ambiguous, outdated, or incomplete.

6.3. The Right to Erasure of Your Data or "Right to be Forgotten"

You can request the erasure of your personal data when one of the following grounds applies:

- Your personal data is no longer necessary for the purposes for which it was collected or processed;
- You withdraw the previously given consent and there is no other legal basis for the processing;
- You object to the processing of your personal data when there is no legal ground for such processing;
- The processing of your personal data is not in compliance with the provisions of applicable legislation and regulations;

Upon a valid request, the Sfil Group will proceed with the erasure of your personal data without undue delay.

However, the exercise of this right to erasure will not be receivable when the retention of your personal data is necessary under legislation or regulation, particularly for the establishment, exercise, or defense of legal rights.

6.4. The Right to Limit the Processing of Your Data

You may request the limitation of the processing of your personal data in the cases provided by legislation and regulation. This means you have the right to request a temporary freeze on the processing of your personal data.

The limitation generally entails the exclusion of any use of your personal data except for the retention of this data, unless you give your consent to another processing operation of your personal data.

6.5. The Right to Data Portability

You have the right to data portability. You have the right to receive the personal data you have provided to the Sfil Group concerning you, in a structured, commonly used, and machine-readable format, and you have the right to transmit this data to another data controller, without the Sfil Group hindering this.

The data on which this right may be exercised includes:

- Only your personal data, excluding anonymized data or data that does not concern you;
- Declarative personal data as well as operational personal data previously mentioned (such as email address, username, age, etc.);
- Personal data that does not infringe on the rights and freedoms of third parties, such as those protected by business secrecy.

This right is also limited to processing carried out using automated processes, based on consent or a contract, as well as personal data that you have personally generated and communicated to us.

This right does not include derived, calculated, or inferred personal data, which are personal data created by the Sfil Group from raw data you have directly provided.

Portability requests are assessed on a case-by-case basis.

6.6. The Right to Object to Data Processing

You have the right to object, on grounds relating to your particular situation, to the processing of personal data concerning you when the processing is based on the legitimate interest of the data controller, including profiling.

The right to object does not apply when the processing is based on a legal obligation.

In case of exercising such a right of objection, the Sfil Group will cease processing these personal data unless there are legitimate and compelling grounds for processing that override the interests, rights, and freedoms of you or for the establishment, exercise, or defense of legal rights.

6.7. The Right to Withdraw Your Consent at Any Time

When the data processing we implement is based on your consent, you can withdraw it at any time. In this case, we will stop processing your personal data without affecting the validity of prior processing operations for which you had consented.

6.8. The Right to Lodge a Complaint and Seek Redress

You have the right to lodge a complaint with a data protection authority (for example, with the CNIL in France) without prejudice to any other administrative or judicial remedy.

CNIL
3 place de Fontenay TSA 80715
75334 Paris Cedex 07
Tel: 01 53 73 22 22

You can make this complaint to the data protection authority in the Member State where your habitual residence, place of work, or the place of the alleged infringement is located.

6.9. Methods for Exercising Your Rights

The Sfil Group provides individuals whose data it processes with the means to effectively exercise their rights regarding this data. All the rights listed above can be exercised at the following email address:

dpo@sfil.fr.

or at the following postal address:

DPO Sfil
112-114, avenue Emile Zola
75015 Paris

However, regarding the exercise of the right to information, we may not be obliged to respond if:

• You already have this information;

• The recording or communication of your personal data is expressly provided for by law;

• The communication of information proves impossible;

• The communication of information would require disproportionate efforts.

For requests other than those regarding the right to information, the individual must prove their identity by clearly stating their first and last name, the address at which they wish to receive a response, and attaching a photocopy of a valid identity document bearing their signature, unless a less intrusive means of verifying their identity is available.

In principle, the individual will obtain access to their personal data free of charge, as well as rectification or erasure, or a response to the exercise of any other rights referred to in Articles 15 to 22 of the GDPR, without undue delay and at the latest within one month from the receipt of the request. If necessary, this period may be extended by two months, taking into account the complexity and number of requests, in which case the individual will be informed of this extension and the reasons for the delay.

When requests from an individual are manifestly unfounded or excessive, particularly due to their repetitive nature, the Sfil Group may:

- Require payment of reasonable fees that take into account the administrative costs incurred in providing the information, making communications, or taking the requested measures, or
- Refuse to comply with these requests.

In the event that any of these requests cannot be fulfilled, the Sfil Group will inform the individual of their right to lodge a complaint with the supervisory authority and to seek judicial redress.

7. Dissemination and Update of This Policy

This Policy is accessible in its current version on the Sfil Group websites.

This policy is regularly updated to take into account legislative and regulatory developments applicable to personal data. To ensure that you always have the latest version, we invite you to consult our websites regularly.

Date of last update: June 2025