POLICY ON PERSONAL DATA PROTECTION

UI efa S.A.

UI efa Policy Reference Number: POL005

June 2025

Table of contents

1. Definitions

Term	Definition
AML/CTF	Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF). Refers to the activities and controls applicable to financial institutions and other regulated entities to prevent and deter money-laundering and terrorist financing.
CISO	Chief Information Security Officer
Client	Any parties, natural person, legal person or legal arrangement, with whom efa has established a contractual business relationship for the provision of services. This includes Third Party Introducers.
CNIL	“Commission nationale de l'informatique et des libertés”, the lead supervisory authority for the protection of personal data in France for the processing operations carried out by efa.
CNPD	“Commission Nationale pour la Protection des Données”, the lead supervisory authority for the protection of personal data in Luxembourg for the processing operations carried out by efa (any request from the CNIL should in principle go through the CNPD, except in exceptional cases).
CSSF	The “Commission de Surveillance du Secteur Financier”, which is the public institution supervising the professionals and products of the financial sector in Luxembourg.
Customer	The “Customer” means collectively: - any Investor and/or Nominee, including UBOs and any person authorized to act on their behalf, that intends to invest or is investing (or is intervening in the investment process) into an Investment Vehicle administered by efa - any Client of efa, including their UBOs.
Data Controller	The natural or legal person, public authorities, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	The natural or legal person, public authorities, agency or other body which processes personal data on behalf of the Data Controller.
Data Protection Coordinator (DPC)	A designated coordinator by the Head of Branch to support the DPO in all data protection aspects in his or her respective jurisdiction, where efa’s branch is located.
Data subject	Any living natural person about whom a Data Controller holds personal data and who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location date, 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.
DPIA	“Data Protection Impact Assessment” is the obligation whereby, where a type of processing operation, in particular through the use of new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller carries out, prior to the processing operation, an analysis of the impact of the envisaged processing operations on the protection of personal data. A DPIA is therefore not necessary for all processing operations and should only be applied to high risk processing operations, according to commonly recognised and accepted criteria.
DPO	Data Protection Officer, as defined in Article 37 GDPR.
GDPR	EU Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
Group	Universal Investment Group (“UI”) and its affiliated entities
Investment vehicle	Any collective investment undertaking (UCI) or other type of investment vehicle, in the Policy also further referred to as “Funds”.
Investor	Natural person or legal person that subscribes in or acquires shares of an Investment Vehicle for which efa provides administration services.
KYC	The term "Know Your Customer" or "Know Your Client" encompasses all work and obligations concerning the knowledge of the Customer and in particular the identification thereof.
Money Laundering	The process by which criminals seek to conceal the illegal origins of the source of their funds generated from criminal activities.
Personal data	Any information relating to an identified or identifiable natural person (hereinafter referred to as 'Data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location date, 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.

Personal data breach	Any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Policy	efa Policy on personal data protection, POL005.
Processing	Any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic 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
Structured data	Data that are captured by used systems of the company. They are generally stored and displayed in organized systems.
Third Party	Any legal entity that is subject to a contractual agreement with efa and (i) receives service provisions from efa and/or (ii) acts as a delegate to efa (meaning that efa is delegating the operation of services in scope of this Policy to a Third Party). For the avoidance of doubt, efa's Clients, Service Providers that provide AML/KYC related services to efa as well as Third-party Introducers are considered to fall under the general term of Third Party and are therefore subject to efa's DD measures.
Third-party Introducer (TPI)	Financial institution or a regulated and supervised entity in accordance with Art. 3-3 of the Law, which transmits orders to subscribe, redeem and transfer units / shares of an Investment Vehicle to efa on behalf of its underlying investors and applies Due Diligence and record keeping requirements in accordance with the Law.
efa	UI efa S.A. and its branches
Unstructured data	Data that are not captured by the system of the company. They are not organized but are stored in easily accessible and shared formats such as e-mails, word and pdf documents, images.

2. Purpose of the Policy

In order for efa to meet its obligations with respect to applicable data legislations, in particular the General Data Protection Regulation 2016/79 (GDPR), this Policy formalizes efa's outline, governance, main principles, procedures and controls in order to maintain the confidentiality, integrity, availability, and security regarding the protection of Personal data.

3. Scope

This Policy applies to all employees of efa, to efa's Supervisory Board, and to any external staff working under a contractual relationship under direct efa's guidance (e.g. consultants, contractors).

This Policy is also directed towards Data subjects whose Personal Data are handled in the course of carrying on efa's commercial activities. These individuals, not limited, could be Customers, prospective Customers or their representatives, agents or appointees, or an employee, director, officer or representative of another organisation with which efa has a business relationship.

The Policy applies to all processing of Personal data, whether automated or not, carried out by efa in the course of its activities, whether acting as a Data Controller or as a Data Processor.

efa acts as:

a) Data Controller for the processing it carries out:

- for the purpose of complying or remaining in compliance with the legal obligations directly applicable to it,
- for the purpose of fulfilling its contractual obligations under its:
    - employment contracts with its employees,
    - service contracts with its Customers, which refers to acts necessary to deliver, manage and invoice the services provided to Customers, with the exception of acts referred to in point b. below, and
    - relationship with its providers for the purposes of billing, service performance, business development.

- for purposes related to its own legitimate interests (e.g. staff appraisal or Customer marketing activities)

b) Data Processor for all processing that it carries out exclusively on behalf of and as appointed delegate of efa's Client (such as the keeping of registers of shareholders of investment funds or the performance of AML/KYC obligations for example).

The guiding principles set forth in this Policy shall also be respected when any activities, in scope of this Policy, are delegated to Third Parties.

4. Relation with existing policies

This Policy is part of a more general framework in relation to efa's data protection laws compliance and is connected with the Compliance Charter (POL013), the Code of Conduct (POL012), the AML/CTF Policy (POL011), the Outsourcing Policy (POL003),Cookie Policy published on efa's website.

5. Risk appetite statement

The Management Board of efa define the risk appetite for the company in the "Risk Strategy of UI efa".

With respect to potential breaches of regulatory requirements, including the violation of data protection laws, the compliance risk has been set as low by the Management Board in the above-mentioned document.

6. Governance

efa's Governance bodies consist of its Supervisory Board , its Audit, Risk and Compliance Committee, its Operational Risk Committee, and its Management Board.

The Audit, Risk and Compliance Committee assists the Supervisory Board with the supervision of internal controls, internal and external audit, risk management and the compliance department. With respect to the protection of Personal data, it shall in particular:

- Acknowledge efa's GDPR Policy and retention schedules.

The Management Board is responsible and accountable for the compliance of all processing operations carried out by efa, whether as Data Controller or Processor. It shall ensure that efa has internal written policies and procedures governing efa's implementation of strategy, principles and its business plan as set forth by. It shall ensure that efa's policies and procedures comply with all applicable laws and regulations and promote good internal governance.

For that purpose, the Management Board shall:

- Review and validate efa's GDPR Policy and any subsequent changes to it;
- Verify that efa's GDPR Policy and any required procedures are properly implemented and non-compliance is promptly corrected;
- Ensure that appropriate management information concerning data protection is provided and used by all required decision-makers within efa; and
- Designate the DPO and support the DPO in performing his or her tasks by proving resources necessary to carry out those tasks and access to personal data, and processing operations, and to maintain his or her expert knowledge.

The Operational Risk Committee is the body that is responsible for taking a position on the GDPR risks identified by the DPO and his or her department. The DPO submits issues, risks and actions to the Operational Risk Committee for advice or decision. When the latter deems it necessary, it submits and escalates these points to the Management Board.

7. Roles and Responsibilities

7.1 All staff are responsible for:

- Knowing, understanding and respecting the requirements contained in this Policy;
- Immediately reporting any incidents or breaches of Personal data to the DPO (and/or his team), see section 9.4 below;
- Participating in and successfully completing training on GDPR;
- Consulting or informing in advance the DPO before implementing any new processing.

7.2 The DPO is responsible for:

The DPO is an independent body in placement and judgment designated by efa as a data controller and data processor. As such, the DPO acts in an independent manner, and involves properly and timely in all issues which relate to the protection of personal data by:

- Informing the Management Board as part of the half-yearly Compliance report; a GDPR section specifies, in particular, the actions taken to comply with the law, or to remain in compliance with the law, as well as any non-compliance events or situations that have been noted or reported to it;
- Informing and advising the Management Board on their obligations under the law;
- Exercising the legal and regulatory watch on data protection, and in particular regularly informing itself of good practices and recommendations from the CNPD or from other experts;
- Coordinating the maintenance of the register of processing activities and the list of sub-processors;
- Being the primary contact point for Data subjects on all matters relating to the processing of their Personal data and the exercise of their rights;
- Controlling through the Compliance monitoring program the respect of the law on data protection (in particular, GDPR);
- Coordinating the organisation of staff awareness and training sessions (as referred to in point 11);
- Advising on the execution of any DPIA and coordinating with the relevant business lines and the CISO, if necessary, and verifying its execution;
- Coordinating the drafting and ensuring the implementation of and compliance with procedures related to the Policy for all efa's activities involving the processing of Personal data[1];
- Cooperating with the CNPD (and where appropriate with other national data supervision authorities) and acting as the main contact point for them on matters relating to the processing of Personal data;
- Taking due account, in the performance of its tasks, of the risk associated with the processing operations having regard to the nature, scope, context and purposes of the processing.

7.3 The CISO is responsible for:

- Defining and ensuring the implementation of adequate technical and organisational security measures to ensure the protection of Personal data against the risks associated with the use of information systems, on the basis of the level of acceptable risk proposed by the DPO likely to impact the persons concerned, validated if necessary by the Management Board or the Operational Risk Committee.
- Keeping a technological watch on all topics related to the security of information systems.
- Assisting, if required, the DPO regarding Personal data breaches and the execution of any DPIA.

7.4 The Compliance Department is responsible for:

- Taking appropriate steps to ensure that any processing of Personal data is carried out in accordance with this Policy;
- Ensuring that the functions and departments concerned involve a member of the Compliance department (under the supervision of the DPO) in a timely manner and provide the information necessary for the exercise of the functions delegated by the DPO (e.g. updating the processing register, procedures);
- In the event that the DPO (and/or team members) is facing a conflict of interest while performing tasks and duties

[1] Any reference to the Policy in this document extends to procedures taken in application of the Policy.

assigned to the DPO (and/or his/her team) by this Policy, ensuring that these latter tasks and duties are performed by other team members.

7.5 The Legal department is responsible for:

- Reviewing any contractual agreements to which efa is party;
- Ensuring that any deviations from standard language for GDPR provisions in efa's agreements is escalated to the Compliance department for review and validation.
- Ensuring that efa's service providers and subcontractors are involved in the processing of Personal data by efa under an appropriate contractual framework that complies with legal requirements so that the processing concerned remains in compliance with the Policy and the law.
- Informing the DPO of any new subcontractors/sub-processor in order for the DPO to update its register of sub-processors accordingly.

7.6 Head of Branches:

- Each Head of efa's branch shall designate a data protection coordinator in his or her respective jurisdiction, who shall closely collaborate with efa's DPO in all issues which relate to the protection of personal data;

8. General Principles

efa is responsible and accountable for any processing activities, hence, it is committed to process Personal data with the following principles:

- process lawfully, in good faith and in a way that is comprehensible to the Data subject ("lawfulness, fairness and transparency");
- collect for specified, explicit and legitimate purposes and not further process in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes in the sense of Article 89(1) ("purpose limitation");
- adequately, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");
- accurately 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");
- 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 the sense of Article 89(1), and subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject ("storage limitation");
- process 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").

8.1 Which Personal data do we process?

The nature of efa's relationship with a Data subject will determine the type of Personal data that are held.

In particular, the data processed might be Structured or Unstructured data and concern:

Categories of Data subjects	Category of Personal data likely to be processed	efa typically acts as
Clients	Group 1	Data Controller
Investors	Group 2	Data Processor
Third Party/Counterparty/Supplier	Group 3	Both
Website visitor	Group 4	Data Controller
efa Employee	Group 5	Data Controller
Job applicants	Group 6	Data Controller

Categories of Personal information efa processes	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6
Full Name	x	x	x		x	x
Address	x	x	x		x	x*
E-mail address (professional)	x	x	x		x	
E-mail address (private)		x			x	x
Specimen signature	x	x	x		x	
Phone number / Mobile phone number	x	x	x		x	x
Occupation/employer	x	x	x		x	x
Date of birth	x	x	x		x	x
Place of birth	x	x	x		x	x*
Gender	x	x	x		x	x
Nationality	x	x	x		x	x*
Information on Source of funds & Source of wealth	x	x				
Bank account details	x	x	x		x	
FATCA-CRS Status, Tax Status,Tax IDs	x	x	x		x	
Passport/ID card	x	x	x		x	
Client ID	x	x	x			
PEP status/adverse media/sanctions	x	x	x		x*	
IP address				x		
Web browser and screen resolution				x		
Operating system and device type (computer, mobile, tablet)				x		
Navigation feed and clicks				x		
Session statistics				x		
Curriculum vitae	x	x			x	x
Criminal record (not kept)					x	
Salary Information					x	x
Diploma					x	x
Pictures	x	x			x	x*
Medical certificate, leave (maternity)					x	
Marital status, name of spouse, number and names of children					x	x
Remuneration data					x	x
Training and further education data					x	x
Logs of entry/exit with employee's number of identification					x	
Working times and teleworking times					x	
Data of leasing if applicable					x	
Pension data					x	
National social security number					x	

* If included in CV

efa may also processes Personal data that has been obtained from publicly accessible sources (e.g. debtor registers, land registers, registers of commerce and associations, press, media) or other sources such as fraud prevention agencies, law enforcement agencies.

efa assumes that electronic files saved on professional electronic devices are professional files except if expressly named "PRIVATE". efa shall not access those private folders except under specific and exceptional circumstances. The employee must be present, the interference with the right to privacy shall be legitimate, justified and, proportionate to the goal pursued.

8.2 Specified purposes for the processing of Personal data by efa

a) **efa is processing Personal data for the purposes of a contractual obligation**

efa processes Personal data in relation to the products and services that it offers, for instance the Data subject's investment in the relevant Fund under administration. In this regard, Personal data may be processed for the following purposes:

- Maintaining the register of shareholders/unitholders;
- Processing subscriptions and redemptions of shares/units and payments of distributions to shareholders/unitholders;
- Maintaining controls in respect of late trading and market timing practices.

In the context of Fund's relevant operations and provisions of services, the Fund might process personal data concerning its contractual counterparties. In that regard, efa may also process data as Data Processor, acting on behalf of the Fund.

efa processes Personal data with respect to the fulfillment of its contractual obligations towards its employees.

b) efa is processing Personal data for compliance with laws and regulations

Investment Vehicles, their Management Company/AIFM, their service providers and any of their affiliates process Personal data in order to comply with various international and domestic legal obligations to which they are subject pursuant to statutory and regulatory requirements.

This includes legislations relating to AML/CFT, KYC, accounting requirements, as well as meeting the demands and requirements and responding to requests and requirements of domestic or foreign regulatory or judicial authorities, tax identification and, where applicable, tax reporting, and any automatic information exchange regime to which the Investment Vehicle and/or their Management Company/AIFM may be subject to.

c) efa is processing Personal data based on the Data subject's consent or for its legitimate business interests

This includes the use and further processing of Personal data with the explicit consent of the Data subjects, for example for the purposes of receiving marketing material, or the application of job candidates.

efa's website and its cookies are mainly resorted to in order to collect Personal data based on your consent. For more information, please consult efa's Cookie Policy published on efa's website.

We may also process biometric data for the sole purpose of the identification and verification of the Customers' identity, with their explicit consent. An alternative will be left to the Customers to proceed via the provision of an identification document.

The processing of video recordings using video conferencing for training and documentation purposes shall be permitted when the data subjects, who are recorded consent to the recording.

The consent may be withdrawn at any time for processes based on the Data subject's consent.

8.3 How long do we keep Personal data?

efa retains Personal data as long as necessary for the purpose for which it is processed, and in compliance with respective legal retention periods applicable.

8.4 Who do we share Personal data with?

Depending on the respective fulfillment of the aforementioned purposes, we may solely disclose your Personal data to:

- UI efa S.A is a member of the Universal Investment Group and when it is acting as the Data Controller in terms of , recruitment, employment or business operations may share the data collected in relation with employment, recruitment and for the purpose of ensuring the continuation of operational activities as well as for internal administrative and managerial purposes on a need to know basis with the Group's entities, as appears from, inter alia, recital 48 of the GDPR;

- UI efa's branches may have access to the data collected in relation with efa's employment and business operations, respectively, efa shall have access to the data collected by its branches in terms of employment or ensuring continuation of operational activities;
- Delegate/Service providers: efa acting as Data Controller or Data Processor may sub-contract to another entity, such as service providers, the processing of Personal data. This might include Cloud service providers under the conditions defined in the Outsourcing Policy (POL003);

  Service providers may also engage sub-processors. Where efa acts as Data Controller and engages subcontractors acting as Data Processors, it shall ensure that such Processors provide sufficient guarantees to implement appropriate technical and organisational measures and that such processing, on behalf of the Data Controller, meets the requirements of GDPR and ensure the protection of the Data subjects' rights. For more information on this issue, please refer to the Outsourcing Policy (POL003);
- Regulated professionals such as lawyers or auditors appointed by efa, its affiliates, delegates or Clients.
- Third party agents and contractors with whom we operate to conduct business;
- Clients may have access to the data in connection with the operations of the Funds;
- Depositary bank and or clearing houses;
- Authorities to the extent permissible by law, as described in section 8.2 (b).

8.5 Transfer of Personal data outside the European Economic Area

Any transmission of Personal data to any aforementioned data recipients, who have their registered office outside of the European Economic Area ("EEA" - third country), is strictly limited to what is necessary. It will only take place to perform our contractual or legal obligations and be in accordance with Article 44 and following of the GDPR.

To provide appropriate safeguards, efa shall perform transfer impact assessment in case of transfer of personal data outside of the EEA and we may rely on an adequacy decision delivered by the European Commission in accordance with Article 45 of the GDPR, or on a standard contractual clause as provided by Article 46 of the GDPR.

In the absence of appropriate safeguards, we will not transfer personal data towards a third country, unless a specific derogation applies in the sense of Article 49 of the GDPR, such as the Data subject's consent prior to the transfer for example.

In the event that you want to obtain a copy of the appropriate safeguards put in place for your data, you can send a written request as stated in section 8.6.

8.6 What are Data subjects' rights regarding their Personal data?

efa is obliged to, and undertakes to, respect the rights of Data subjects as conferred on them by law.

Each Data subject has the right:

- To information on the processing operations for which their data are involved,
- To access and rectify their data,
- To oppose to processing,
- To erase their data (right to be forgotten) pursuant to Article 17 of the GDPR,
- The right to restriction of processing in accordance with Article 18 of the GDPR,
- The right to withdraw his/her consent (if data are processed based on the consent of the Data subject)
- The right to data portability, when feasible, in accordance with Article 20 of the GDPR.

To make any of the above requests, Data subjects need to put the request in writing, addressing it to the Data Processing Officer, who can be contacted by email at "dpo@efa.eu" or by post at the following address:

UI efa S.A.
Data Protection Officer
2, Rue d'Alsace
L-1122 Luxembourg
Grand Duchy of Luxembourg

efa may refuse to exercise the data subject's rights which are mentioned above when it is not in position to identify the Data subject and shall inform the Data subject to provide additional information enabling his or her identification in the sense of Article 11(2) of the GDPR.

Data subjects have the right to lodge a complaint with the Luxembourg “Commission Nationale pour la Protection des Données” (“CNPD”) or the relevant authority of the Member State in which the Data subject resides or works in accordance with the provisions of Article 77 of the GDPR.

Commission Nationale pour la Protection des Données (CNPD)
15, Boulevard du Jazz
L-4370 Belvaux
Grand Duchy of Luxembourg
Tel.: (+352) 26 10 60-1, website: cnpd.public.lu

9. Procedures for the protection of Personal data

9.1 Maintaining of a record/register of processing activities.

efa shall keep an up-to-date record of all processing activities carried out as the Data Controller and Data Processor. The head of branch, department or function concerned shall maintain a record of processing activities. The DPO is responsible for ensuring the maintenance and regularly reviewing the register. The register shall contain at least the legal information required by Article 30 of the GDPR.

For each new processing activity, the branch, department or function concerned by the processing operation completes the register and where is necessary with the assistance of the DPO (and/or his/her team) . The head of the branch, department or function shall be responsible for accuracy of the register and provides the list of processing activities concerned to the DPO (and/or his/her team) on timely and regular basis by providing him/her with the necessary information (in particular and without limitation concerning data transfers outside the European Union, and/or to Processors).

Record of processing activities is kept by the DPO (and/or his team) and ensures that the record/register is made available to:

- the CNPD and the CNIL where applicable, in the cases provided for by law,
- the Operational Risk Committee, the Management Board and the CISO for all processing.

9.2 Checking the Compliance of processing activities.

The DPO (and/or his team) checks before (as far as possible) the start of any new processing activities, and regularly for all existing processing operations:

- compliance with the principles of lawfulness, fairness, transparency, purpose, data quality, legitimacy and proportionality of processing;
- that the information collected are limited to what is strictly necessary ("data minimisation" principle) and collected for specified, explicit and legitimate purposes (“purpose limitation” principle);
- that the data is destroyed (together with the corresponding archives) when its retention is no longer necessary; it is the responsibility of the Management Board to validate the applicable retention periods for each type of data and each processing. Proposals should be made by the DPO after verification with the relevant departments including Legal and Compliance.
- that data are 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’).

9.3 Data protection impact assessment (“DPIA”)

When efa is acting or defined as the Data Controller, it shall perform a DPIA prior to processing any Personal data by taking into account:

- Nature;
- Scope;
- Context; and
- Purpose of the processing activities.

DPIA is a risk management and mitigating tool to demonstrate compliance with the GDPR. In light of this, the person in charge of the processing activity or project, shall perform a preliminary data impact assessment based on the following criteria in the sense of recital 91 of the GDPR:

- Processing activity would lead to evaluation or scoring of Data subjects;
- Processing activity would lead to an automated decision making with legal or similar significant effect;
- Processing activity is regarding the systematic monitoring;
- Processing sensitive data or data of a highly personal nature;
- Processing of a large scale of data;
- Processing through matching or combining datasets;
- Processing personal data of vulnerable Data subjects;
- Applying new technological or organizational solutions;
- Processing in itself would prevent Data subjects from exercising their right or using the service or contract.

In case two or more of these criteria would meet the type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, efa's staff shall carry out data protection impact assessment of the envisaged processing operations.

Where the preliminary impact assessment results unclear, whether the DPIA is required, efa shall carry out data protection impact assessment. In some cases, where the processing activity meets only one of the above criteria, efa may consider carrying out a DPIA.

In the event that an impact assessment has not yet been carried out, such as in case of new processing of Personal data, the DPO shall be made aware by the Head of the relevant branch or department of the new process and shall assess whether a DPIA is necessary.

In the affirmative, the DPIA should be carried out by the head of the relevant branch or department under the supervision of the DPO and the assistance of the CISO. The DPO will create and maintain a record of processes subject to a DPIA.

efa shall consult the Supervisory Authority where a DPIA results in a high risk in the absence of measures taken to mitigate the residual high risk.

9.4 Personal Data Breaches

In the event of a Personal data breach, efa must comply with its legal obligations as described below, and deal with the incident in a way that limits its impact on Data subjects and avoids its recurrence.

The DPO (and/or his/her team) should be informed immediately of the existence of such a breach, should be kept informed of any further developments and should be provided with any relevant factual information about the incident. The DPO may require the assistance of the CISO depending on the importance and nature of the breach.

The DPO (and/or his/her team) shall keep a record of any Personal data breach, indicating its context, the facts, effects of the incident and the measures taken to remedy the breach.

a) If efa is acting as Data Controller for the processing concerned, the DPO (and/or his team):
   - Coordinates the notification of the Personal data breach to the CNPD (which refers it to the CNIL if necessary) as soon as possible and, unless justified, no later than 72 hours after the discovery of the incident (unless the breach in question is not likely to give rise to a risk to the rights and freedoms of the persons concerned);
   - Ensures that the notification complies with the law and contains all the information required by it;
   - Advises the Operational Risk Committee (convened as a matter of urgency) on whether or not to inform the Data subjects, so that this Committee can take a decision on the matter;

b) If efa acts as a Data Processor of a Client (who is Data Controller) for the processing concerned, the DPO (and/or his team):
   - Shall notify the Client of the Personal data breach and efa shall assist the Client in accordance with the law. In this case, the Client is responsible for the notification process with the authorities or to the Data subjects.

10. Controls and monitoring

The DPO shall monitor compliance with the relevant national and European data protection legislation. The DPO shall be equipped with sufficient resources and capacity available to carry out these activities. In addition to monitoring compliance with data protection legislation, the DPO also shall monitor internal compliance with this Policy.

To ensure risk-oriented monitoring of privacy and data protection management, recurring checks and audits shall be carried out in line with Compliance's monitoring plan. The results of the monitoring will provide a clear picture of efa's data processing and protection status, and implementation depth for each area of investigation.

Regular reports by the DPO are an important tool for demonstrating compliance with general principles and for proving accountability. For this reason, data protection reports shall be prepared by the DPO at least once a year and is made available to the Management Board. Based on the DPO's assessments, a final overall risk classification of the company shall be made by the Management Board. This risk classification shall form the basis for prioritizing ongoing, risk-minimizing measures for the continuous improvement process in data protection.

11. Training and communication of changes to the Policy

efa is committed to strengthening the information security and data protection culture within all its departments.

efa is committed to updating the Policy and the procedures and guidelines derived from it in order to take into account legal, regulatory or technological developments as well as the operational constraints of the services. Any changes made to this Policy will be posted on efa's website.

efa's employees have to participate to ongoing training programs related to data protection laws.

The purpose of the program is to inform or remind relevant staff about the up-to-date status of the following topics:

- Content of GDPR regulations and Law and subsequent, duties, obligations and responsibilities on efa and efa staff;
- efa's GDPR policies and procedures;
- Practical examples and use cases of operations that could typically be related or point out GDPR issues, providing guidelines and instructions on how to proceed if such issues occur.

According to the function occupied, staff will be trained on a regular basis and made aware of the applicable GDPR regulations and relating duties.

12. Applicable Laws and Regulations

EU Regulation 2016/679 of 27 April 2016	Protection of natural persons with regard to the processing of Personal data and on the free movement of such data (GDPR).
Directive 2002/58/EC of 12 July 2002	Concerning the processing of personal data and the protection of privacy in the electronic communications sector.
Law of 30 May 2005	Relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et - portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.
Law of 1st August 2018	Portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État.
Law of 12 November 2004	On the fight against money laundering and terrorist financing transposing Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering and amending (...)

Law of 24 July 2015	Portant approbation de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des Etats-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et relatif aux dispositions des Etats-Unis d'Amérique concernant l'échange d'informations communément appelées le «Foreign Account Tax Compliance Act», y compris ses deux annexes ainsi que le «Memorandum of Understanding» y relatif, signés à Luxembourg le 28 mars 2014 ; de l'échange de notes y relatives, signées les 31 mars et 1er avril 2015. (FATCA)
Law of 18 December 2015	Concernant l'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale et portant : transposition de la directive 2014/107/UE du Conseil du 9 décembre 2014 modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal ; modification de la loi modifiée du 29 mars 2013 relative à la coopération administrative dans le domaine fiscal. (CRS)

13. Ownership and document approval

Version history	Description of changes	Date of document	Written or updated by	Date of validation by Management Board	Date of acknowledgement by ARC Committee	Date of acknowledgement by Supervisory Board	Target audience
V1.0	Creation of the GDPR policy	10/09/2018	Compliance		-	-	
V2.0	Update of Personal data protection Policy & translation in English.	01/09/2022	Compliance	22/09/2022		-	
V3.0	Update of the name of efa and changes in order to align with the new Policy template, alignment with UI group standards	20/11/2023	Compliance	21/11/2023	29/11/2023	15/12/2023	
V4.0	Annual review	23/05/2024	Compliance	29/05/2024	05/06/2024	18/06/2024	
V4.1	Annual review Update of CNPD address Type of change[2] ☒Editorial ☐Technical	17/06/2025	Compliance	27/06/2025	-	02/07/2025	All UI efa

This Policy is approved by UI efa's Management Board and acknowledged by the ARC Committee and UI efa's Supervisory Board.

The DPO shall review and, if required, update the Policy at least on an annual basis and on an ad-hoc basis if necessary.

For any questions or comments in relation to the information contained in this document please contact the Policy owner as shown below:

Function: DPO
Department: Compliance

[2] **Type of change** : technical or editorial
Technical change: a substantial adjustment of content which is marked by a new "valid-from" date. Validated by the concerned head of departments.
Editorial changes: do not affect the technical content and so do not entail a fresh "valid-from" date, e.g., rewording (wording is altered, but not the intended meaning), changes in references (links, paragraphs), alteration of text sequence, inclusion of genders, correction of spelling errors, renaming, etc., release by owner of the procedure.

14. Confidentiality level

A short version of this Policy can be made available to external parties on UI efa's website.

The short version does not include sections related to Governance (section 6), Roles and Responsibilities (section 7) and to the process of Personal data belonging to efa's employees (mostly section 8).

The short version of the Policy is not confidential and intended for efa's internal and external use of efa's job applicants, Customers and other business partners. The document is the property of efa, and must not be copied or used for any purposes other than that for which is it supplied. efa's Customers or other counterparties may review a copy of this document on site or through a publicly available electronic access.