Europ Assistance Holding

EUROP ASSISTANCE PUBLIC PRIVACY GROUP POLICY

EAH Compliance

EA Policy

Public version

EXECUTIVE SUMMARY

This Personal Data Protection Policy (Policy) supports the implementation of the EU General Data Protection Regulation no. 679/2016 (GDPR) across Europ Assistance Group (EA) and sets the minimum requirements that any EA Legal Entity – which may be under the scope of the GDPR, UK GDPR or Swiss data protection law – must implement when processing personal data.

This Policy applies whether an EA Legal Entity acts as a Data Controller or as a Data Processor. It applies to any processing of Personal Data, irrespective of the nature or category of the Personal Data processed, regardless of the medium in which Personal Data is stored.

INDEX

Glossary and definitions

Acronym/Term	Explanation/Definition
Data Controller	The individual or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Processing	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Processor	The individual or legal person that processes the Personal Data on behalf of the Data Controller.
Data Protection Impact Assessment or DPIA	An assessment of the impact of the envisaged Processing operations on the protection of Personal Data to be carried out by the Data Controller when a 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 individuals.
Data Subject	An identifiable individual is one who can be identified, directly or indirectly, in particular by reference toan 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.
EA Legal Entity	Any company/subsidiary/branch of a company under the control of Europ Assistance Holding, the parent company of Europ Assistance Group.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council 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 and repealing Directive 95/46/EC (General Data Protection Regulation).
Local data protection law(s)	GDPR, Swiss Federal data protection Act, UK GDPR or any other applicable relevant law applicable to a specific territory
Personal Data	Any information, directly or indirectly, relating to an identified or identifiable individual (*i.e.*, Data Subject).
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Special Categories of Personal Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying an individual, Personal Data concerning health, or concerning a natural person's sex life or sexual orientation.
Supervisory Authority	Any independent public authority which is responsible for monitoring the application of Local data protection laws.
Swiss data protection law	The new Federal Act on Data Protection (nFADP) of 25 September 2020, which will come into force on September 1, 2023.
UK GDPR	The General Data Protection Regulation has been kept in UK law as the "UK GDPR". The 'UK GDPR' sits alongside an amended version of the Data Protection Act 2018.

1. INTRODUCTION

1.1 Objectives

Europ Assistance Group (hereafter Europ Assistance or EA) considers Personal Data as a core asset to be safeguarded. Caring for Personal Data according to the most stringent global practices is an essential part of EA strategies towards customers, employees, business partners and all other stakeholders. The purpose of this EA Public Privacy Policy is to share with our stakeholders the key requirements followed by EA entities when Processing Personal Data of European Residents and/or in the European Economic Area (EEA)

1.2 Scope

This Policy sets out the common general principles to be applied and minimum requirements to be implemented by all EA Legal Entities established in the European Economic Area (EEA) with respect to the Processing of Personal Data. The Policy also applies to EA Legal Entities not established in the European Economic Area in so far as they:

(a) offer goods and services to individuals who are in the EEA or,

(b) monitor their behaviour if the behaviour takes place within the EEA.

This public privacy policy is also applicable in the United Kingdom and in Switzerland, given that both countries have similar general principles and requirements in their Local data protection laws.

2. KEY PRINCIPLES GOVERNING PERSONAL DATA PROCESSING

EA Legal Entities apply the following key principles to Personal Data Processing:

- **lawfulness, fairness and transparency**: identify valid grounds (known as a "legal basis") for the Processing and provide individuals with transparent and clear information on how, why, how long and by whom his/her Personal Data will be processed, usually through a privacy notice. Processing Personal Data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned is not allowed;

- **purpose limitation**: collect Personal Data only for specified, explicit and legitimate purposes. Further Processing incompatible with those purposes is not allowed;

- **minimization**: process only Personal Data strictly necessary to pursue the purposes for which they are collected;

- **accuracy**: do not process inaccurate Personal Data and, where necessary, keep Personal Data up to date; when it is discovered that Personal Data are inaccurate, in respect of the purposes for which they are processed, EA Legal Entities must take reasonable steps to correct or erase them without delay;

- **storage limitation**: keep Personal Data for no longer than necessary for the purposes for which they are processed; define and implement a retention period. The duration of the retention period is set on the basis of the purposes of the Processing to the extent that it does not conflict with other local applicable laws and regulations. Following the expiration of the retention period, Personal Data can be retained only in a form which does not permit the identification of the individuals. To implement this principle technical measures to irreversibly de-identify Personal Data, which include deletion, obfuscation, redaction, anonymization, must be adopted;

- **integrity and confidentiality**: ensure that appropriate organizational and technical measures are in place to protect Personal Data, so to avoid un-authorized or unlawful Processing, accidental loss, destruction or damage.

The Data Controller is responsible for compliance with the principles above and must be able to demonstrate at all times (known as the “accountability” principle) through the adoption of appropriate internal regulations, processes and other measures which can include, at a minimum, keeping a record of processing operations, performing a Data Protection Impact Assessment, and performing controls to verify the status of implementation of the Personal Data protections principles and requirements.

An EA Legal Entity, acting in an insurer or reinsurer capacity, will always be considered Data Controller.

When acting as a Data Processor, EA Legal Entities comply with the relevant principles above and ensure that they process Personal Data solely in accordance with the documented instructions of the Data Controller.

3. KEY REQUIREMENTS GOVERNING PERSONAL DATA PROCESSING

Considering the above principles, different key requirements must be implemented depending on whether Personal Data are being processed by an EA Legal Entity acting as Data Controller or as Data Processor.

Both the Data Controller and the Data Processor provide the personnel who Process Personal Data with appropriate instructions and regular training to ensure that Personal Data are processed in compliance with this Policy and the applicable Local data protection laws.

3.1 Key requirements for EA Legal Entities acting as the Data Controller

Whenever, as regards a specific Processing of Personal Data, EA Legal Entities act as **Data Controller,** the activities listed under this Section are carried out.

3.1.1 Process Personal Data on the basis of legal grounds

Processing of Personal Data is lawful when it is:

- based on consent given by the individual for one or more specific purposes; or
- necessary for the performance of: (i) a contract to which the individual is party, or (ii) pre-contractual activities; or
- necessary for compliance with a legal obligation to which the EA Legal Entity is subject; or
- necessary to protect the vital interests of the Data Subject or of another individual; or
- necessary for the performance of a task carried out in the public interest or in the exercise of an official authority; or
- necessary for the purposes of a legitimate interest pursued by the EA Legal Entity, except where such interests are overridden by the interests or fundamental rights and freedoms of the individuals which require protection of Personal Data.

3.1.2 Process Special Categories of Personal Data

EA Legal Entity shall not process Special Categories of Personal Data, except when kept to a minimum:

- based on the explicit consent given by the individual for one or more specific purposes except where applicable laws and regulations provide a prohibition that cannot be lifted by the individual;
- necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the individual in the field of employment and social security and social protection law in so far as it is authorised by applicable law;
- necessary to protect the vital interests of the Data Subject or of another individual where the Data Subject is physically or legally incapable of giving consent;
- necessary for the establishment, exercise or defence of legal claims;
- necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of applicable laws and regulations or pursuant to contract with a health professional and subject to the following conditions and safeguards referred: those Personal Data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under applicable laws and regulations or by another person also subject to an obligation of secrecy under applicable laws and regulations;
- performed in accordance with applicable laws and regulations, including further conditions and limitations regarding the processing of Special Categories of Personal Data. For instance, some countries have introduced other Special Categories of Personal Data (e.g., social security number in France and Luxemburg) or stricter conditions regarding the processing of genetic data, biometric data or health data (e.g., regarding hosting).

On a day-to-day basis, EA Legal Entities collect and process Personal Data for different purposes and on different legal grounds; please find some examples below:

Legal basis	Processing activities
*To execute a **contract***	- perform eligibility checks - manage claims and complaints - insurance underwriting and risk management - policy underwriting and administration - employees' administration
*To fulfill EA's **legitimate interests**,*	- perform fraud prevention or/and prevent irregularities - conduct customer satisfaction surveys - continuously improve the efficiency and the rapidity of EA claim management system (e.g., perform analytics, improve the user experience; debug and conduct research; provide customer service and training) - reinsurance purpose - perform statistical purpose
*To comply with **legal obligations***	- fight against money laundering, - fight against the financing of terrorism, - comply with international economic and financial sanctions
*We also collect **consent***	When collecting sensitive data, such as health and medical data, EA Legal Entities require express consent.

For more details about EA Legal Entities processing activities as a Data Controller, please consult Appendix 1.

3.1.3 Provide the Data subjects with proper information relating to the Processing of Personal Data

Where relevant, EA Legal Entities provide individuals with an adequate, transparent and clear privacy notice relating to the Processing of their Personal Data.

Further details for specific Processing activities are made available by EA Legal Entities in the relevant privacy information notices.

3.1.4 Facilitate the exercise of Data Subjects' rights

Subject to local applicable law, an individual is entitled to exercise the following rights:

a) **Right of access:** right to obtain confirmation as to whether or not his/her Personal Data are processed and, where that is the case, access to the Personal Data;

b) **Right to rectification:** right to obtain the rectification of inaccurate or incomplete Personal Data concerning the individual;

c) **Right to erasure (right to be forgotten):** right to obtain the deletion of their Personal Data, under certain conditions;

d) **Right to restriction:** right to obtain the limitation of the Processing activities on his/her Personal Data. Once restricted, Personal Data can only be stored, unless specific exemptions apply;

e) **Right to data portability:** right to receive his/her Personal Data in a structured, commonly used, and machine-readable format and have those Personal Data transmitted to another Data Controller;

f) **Right to object:** the right to oppose, on grounds relating to their specific situation, at any time to the Processing of Data Subjects' Personal Data. Once the right to object has been exercised, Personal Data must no longer be processed unless the existence of legitimate grounds that override the interests, rights and freedom of the individual, or the need to establish, exercise or defend legal claims is demonstrated. In any case, if the individual objects to Processing for direct marketing purposes, Personal Data must no longer be processed for such purposes.

g) **Right not to be subject to a decision based only on automated processing:** the right not to be subject to a decision based only on automated processing, including profiling, which produces legal effects concerning or significantly affecting them.

h) **Right to withdraw consent:** the right to withdraw their consent, at any time, for the processing of their personal data for which they have provided consent. Withdrawing consent may imply that an EA Legal Entity may no longer be able to proceed with a request.

i) **Right to lodge a complaint**: the right to bring their claim, if they feel an EA Legal Entity has not addressed properly a data protection request, to a supervisory authority. For these purposes, they can contact the competent supervisory authority of their country of residence or the authority of the EA Legal Entity concerned.

EA Legal Entities timely answer the individuals' requests, free of charge, without undue delay.

3.1.5 Ensure that data protection is built in by design and by default

The Data Controller ensures that Personal Data protection is embedded by design and by default.

The Data Controller identifies and implements appropriate technical and organizational measures in order to meet GDPR requirements and protect the rights and freedoms of individuals; such activity is performed at the time of the determination of the means and purpose of any system, service, product or process and at the time of the Processing itself (known as “privacy by design”).

For the identification of the appropriate technical and organizational measures, the Data Controller takes into consideration at least the following:

- the technical and technological solutions available on the market at the time;
- the cost of implementation;
- the nature, scope, context and purposes of the Personal Data Processing; and
- the impacts of the Personal Data Processing on the rights and freedoms of the individuals.

Appropriate technical and organizational measures must ensure, by default, that only Personal Data which are necessary for each specific purpose are processed, the same with reference to the amount of Personal Data collected, the extent of their Processing, their retention period and their accessibility (known as “privacy by default”).

3.1.6 Keep records of the Personal Data Processing activities

Subject to applicable local law, each EA Legal Entity, acting as Data Controller, keeps a record of Personal Data Processing activities performed under its responsibility. It is made available, on request, to the Supervisory Authorities.

3.1.7 Implement adequate technical and organizational measures to ensure a level of security appropriate to the risk

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of likelihood and severity for the rights and freedoms of individuals, EA Legal Entities adopt a risk-based approach and implement appropriate technical and organizational measures in order to ensure an appropriate level of security of customers, employees and the data of our business partners.

EA Legal Entities are committed to effectively managing the increasing complexity of security-related risks by adopting a “One-Security” approach, based on a strong integration between information & cyber and physical & corporate security. This approach leads to the integration of processes and tools for the identification, evaluation and management of security risks and to an increasing resilience against adverse events. More specifically, EA Legal Entities pledge to:

- protect the entity’s ecosystem and strengthen its security standards
- define internal security regulations and monitor their implementation
- define a solid management process for IT and security-related risks
- ensure the implementation of security measures for the management of security and data protection related threats
- raise awareness and understanding around the issue among all employees

EA Group has developed a security awareness program for all our employees which consists of various initiatives such as dedicated training courses, videos and ad hoc communications, together with internal campaigns simulating phishing attacks.

The Group Chief Security Officer oversees the security within EA Group, identifying and implementing the Group security strategy, managing the security budget and regularly reporting on security to the Board of Directors. To strengthen IT security risk management, the Group Chief Security Officer, in coordination with the Group risk management department, has set up a unit specifically dedicated to monitoring and managing cyber risk.

Moreover, EA Legal Entities abide by Generali Group security policies and standards, which are available here.

3.1.8 Notify to the Supervisory Authority and communicate to the Data Subjects a Personal Data Breach

EA Legal Entities have put in place adequate procedures and processes to ensure the proper management of any Personal Data Breaches, including the prompt notification to the relevant Supervisory Authority, unless the Breach is unlikely to result in a risk to the rights and freedoms of individuals and, where relevant, the communication to the affected individuals.

Furthermore, any Personal Data Breach are properly documented and the documentation will be made available to the Supervisory Authority on request.

3.1.9 Carry out an assessment of the Processing impact on the protection of Personal Data (Data Protection Impact Assessment – DPIA)

When required, at the occurrence of specific triggers and subject to local Supervisory Authority guidance, a Data Protection Impact Assessment is carried out for processing operations that are likely to result in a high risk to the rights and freedoms of individuals. The DPIA is aimed at:

- describing the Processing of Personal Data;
- assessing the necessity and proportionality of such processes with regards to the relevant purposes;
- managing the risks for the rights and freedoms of individuals that may arise in connection with such Processing; and
- implementing, where necessary, additional measures to address the risks, including safeguards, security measures and mechanisms to ensure Personal Data are protected.

3.1.10 Frame international transfers of Personal data

The Data Controller ensures that any transfer of Personal Data outside the European Economic Area (EEA), UK or Switzerland is performed in accordance with local laws.

The Data Controller ensures it has adopted at least one of the following recommended safeguards and, where necessary, the supplementary measures appropriate to ensure that the Personal Data transferred receive, in the non-EEA country of destination, a level of protection essentially equivalent to the one provided in the EEA. Preference is to be given to Processing taking place inside the EEA, UK or Switzerland.

Preference must be given to the safeguards in the following order:

- the non-EEA Country ensures an adequate level of Personal Data protection as assessed by the European Commission[1]. The effect of such a decision is that personal data can flow from the European Union (and Norway, Liechtenstein and Iceland), UK or Switzerland to that third country without any further safeguard being necessary; or
- standard contractual clauses[2] for the transfer of personal data to third countries (SCCs) adopted by the European Commission are signed; or
- transfer is necessary for the performance of a contract between Data Controller and Data Subject; or
- transfer is necessary for the establishment, exercise or defence in a legal claim; or
- Data Subject explicitly consents to the specific Personal Data transfer; or
- in specific situations as regulated under Local data protection law, e.g., where the transfer is not repetitive and concerns only a limited number of Data Subjects, it is necessary for the purposes of compelling legitimate interest pursued by the EA Legal Entity, provided that all circumstances have been assessed and the Data Controller has adopted all necessary safeguards for the Processing.

When the transfer to a non-EEA country is based on standard contractual clauses (SCCs) adopted by the European Commission, the Data Controller has to assess whether they are effective in light of all the circumstances of the transfer and, if not, the Data Controller must adopt additional legal, technical or organizational measures (e.g., encryption in transit and at rest, end-to-end encryption, anonymization, pseudonymization) to ensure that the Personal Data transferred are afforded in the third country a level of protection essentially equivalent to that guaranteed in the EEA, UK or Switzerland.

If no safeguard is applicable and/or if no additional measure appears to be effective to ensure that the Personal Data transferred will be afforded, in the third country of destination, a level of protection essentially equivalent to that guaranteed in the EEA, UK or Switzerland, or whenever in doubt, the Data Controller will refrain from transferring Personal Data.

EA Legal Entities are aware that the cross-border Personal Data transfer provisions apply not only to transfers of Personal Data to third parties (e.g., to suppliers, vendors) but also within EA Legal Entities and sign proper agreements among EA Legal Entities in order to comply with article 28 GDPR.

3.1.11 Give documented instructions to any third party acting on behalf of the Data Controller

When the Data Controller delegates the Data Processing to a third party (outside or within the EA Group), the Data Controller must appoint a Data Processor in writing.

EA Legal Entities enter into contracts with all internal and external Data Processors, which includes the duty to follow the documented instructions of the Data Controller and implement appropriate technical and organizational measures. The Data Controller must authorize any appointment by the Data Processor of sub-Data Processors. The prior written authorization can be

[1] European Commission Adequacy decisions (europa.eu)
[2] For the UK, the term "standard contractual clauses" refers to the international data transfer agreement (IDTA), the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (Addendum) and a document setting out transitional provisions.
For Switzerland, the term "standard contractual clauses" refers to the standard data protection clauses approved, issued or recognized by the Federal Data Protection and Information Commissioner in accordance with Article 16 of Swiss Federal Act of 25 September 2020 on personal data protection.

general or specific.

3.1.12 Carry out due diligence & audit

EA Legal Entities carry out due diligence before engaging in a new relationship with a third party.

Focusing on the whole supply chain management and on outsourcing activities, EA Legal Entities have proper processes and tools for the identification, evaluation and management of third parties processing Personal Data. Before a Data Processor is appointed, the Data Controller must ensure that the Data Processor has in place appropriate technical and organizational measures capable to comply with the Personal Data principles and requirements as well as the exercise of Data Subjects' rights.

EA Legal Entities follow a risk-based approach, adopting a proportionality principle to apply requirements according to the risk profile, the materiality of each outsourcing agreement and the extent to which they control the service providers.

EA Legal Entities also conduct audits and inspections, of relevant Data Processors either themselves or conducted by another auditor mandated by them.

Within EA Group, EA Legal Entities have data protection audits on a regular basis in coherence with their specific situation and the principle of proportionality. In addition to the regular audits, specific audits (ad hoc audits) may be requested by the Data Protection Officer (DPO), a Local Data Privacy Correspondent (DPC) or any other competent function in the organization, to ensure verification of compliance with this Privacy Policy.

3.2 Key Requirements for entities acting as the Data Processor

Whenever, as regards to a specific Processing of Personal Data, an EA Legal Entity acts as **Data Processor**, taking into account the nature of the specific Processing and the information available to the Processor, it:

- signs a contract or other legal act governing the relationship with the Data Controller;
- processes Personal Data only according to the documented instructions of the Data Controller, unless otherwise required by applicable laws;
- processes the Personal Data in accordance with the relevant principles set out in this Policy and the applicable Personal Data protection laws and regulations;
- ensures that individuals authorized to process the Personal Data have committed to confidentiality or are under an appropriate obligation of confidentiality;
- maintains a record of all the Processing activities; When acting on behalf of a Data Controller, the Data Processor establishes and maintains a dedicated record for each of the Data Controllers;
- implements appropriate technical and organizational measures to protect the Personal Data Processing, as agreed with the Data Controller;
- appoints a Data Protection Officer or a Local Data Privacy Correspondent (DPC), if required;
- refrains from appointing another Data Processor without the prior authorization of the Data Controller. In case the Data Processor has received a general written authorization to engage other Data Processors, it shall timely inform the Data Controller of any intended changes concerning the addition or the replacement of other Data Processors, in accordance with the relevant agreement;
- whenever the Data Processor engages Data Sub-processors for carrying out the specific Processing activities on behalf of the Data Controller, signs a contract with this Sub-processor to impose the same Data Protection obligations set out in the contract with the Data Controller; the initial Processor remains fully liable to the Data Controller for the performance of other processor's obligations.
- assists the Data Controller in meeting its obligations with respect to the responding of requests related to the rights of Data Subjects;
- assists the Data Controller in meeting its obligations by co-operating in a timely manner with any DPIA undertaken by the Data Controller and in fulfilling any obligations to engage in prior consultation with the relevant Supervisory Authority;
- provides notification, without undue delay, to the Data Controller in relation to any Personal Data Breach or incident impacting the Personal Data being processed on behalf of the Data Controller;
- after the termination of the provision of services, returns or deletes existing copies of Personal Data, at the request of the Data Controller, unless Union or local applicable law requires storage of the Personal Data; and
- makes available to the Data Controller all information necessary to demonstrate compliance with its legal obligations as Data Processor and allows for and co-operates with audits, including inspections, conducted by the Data Controller or another auditor appointed by the Data Controller, in accordance with the relevant agreement.

4. DATA PROTECTION GOVERNANCE

Organization

Whenever acting as Data Controller or Data Processor, and where required under Local data protection law, the EA Legal Entity appoints a Data Protection Officer (DPO) or a Local Data Privacy Correspondent (DPC).

The DPO function can be outsourced to other EA Legal Entities or to third parties.

For coordination and consistency purposes, Europ Assistance has decided to appoint one Data Protection Officer at Group level which acts as DPO for all relevant Europ Assistance Legal Entities and to create a network of local Data Privacy Correspondents (DPC).

The EA Group Data Protection Officer guarantees guidance and coordination of the Local Data Privacy Correspondents of all EA Legal Entities. The Group DPO provides guidelines and operating procedures for the implementation of Personal Data related policies to the DPCs who customize them to local laws, regulations and organization.

At local level, the Data Privacy Correspondents (DPC) play a key role in fostering the implementation of the applicable laws and regulations on Personal Data protection and in facilitating their compliance, e.g., handling local complaints from data subjects, reporting major privacy issues to the Group DPO, monitoring training and compliance at a local level.

Training

EA Legal Entities ensure appropriate and up-to-date training on data protection is provided to employees who have permanent or regular access to personal data, who are involved in the collection of data or in the development of tools used to process personal data.

Effective Date

The Policy is effective as of 1 October 2023.

The Policy shall be reviewed on a regular basis, especially to include developments in legislation, market and/or best practices, Europ Assistance strategy and organization.

Do you have any questions about this Policy?

Contact us at: eaglobaldpo@europ-assistance.com or by mail: Europ Assistance Holding, à l'attention du DPO, 2 rue Pillet-Will 75009 Paris

APPENDIX 1: EA LEGAL ENTITIES PROCESSING ACTIVITIES AS A DATA CONTROLLER

Data subjects concerned

As part of day-to-day business operations, EA Legal Entities may collect and process Personal Data relating to:

- Job candidates,
- Employees and former employees,
- Employees of agents brokers and distributors
- Policyholders
- Beneficiaries and insured
- Clients and prospects,
- Employees of the business partners,
- Employees of the service providers and suppliers,
- Any other third party.

Personal data processed

Depending on the interaction EA Legal Entities may have with the Data subjects listed above, EA may collect and/or process the following categories of personal data:

- Identity and contact information (e.g., name, date of birth, gender, address, passport)
- Demographic data & Personal life data
- Professional life data (e.g., employee number, salary, performance at work, annual evaluation, job title & company)
- Economic and financial data (e.g., bank account, economic situation)
- IT Logging, traffic and tracking data (e.g., IP address, cookies, electronic communications, Internet searching history)
- Data related to geolocation and movements (e.g., data extracted from black boxes, GPS),
- Any data which may be relevant to assess insurance claims (including medical and health data, social security number)
- Any relevant data provided to EA in the contact forms /help center
- Criminal convictions and offences

Personal data processing activities

EA Legal Entities may process Data subjects' personal data for the following purposes:

- **Insurance for travel, auto and home & family business lines**: eligibility checks performance; claims and complaints management; insurance underwriting and risk management; policy underwriting and administration;
- **Travel assistance services:** travelers support, assistance & repatriation;
- **Road assistance services:** roadside assistance;
- **Medical teleconsultation** service (or medical advice, depending on local regulations); healthcare journey solution;
- **Concierge services**: manage customers requests & business partnerships
- **Home & family assistance:** teleassistance; handle emergency interventions, protect homes, deliver personalized care and assistance to families; Identity theft protection
- **HR**: career opportunities management; general management of employees, performance management, career development, health and safety compliance, sickness monitoring/compliance, diversity monitoring, disciplinary procedures, security checks (if and where required), visa applications and other immigration requirements,…
- **Corporate Finance, Mergers and Acquisitions**
- **Finance**: payroll, pension, shares and similar services in relation to employment obligations and employees benefits
- **Marketing & communications**: information & promotion of Europ Assistance`s products or services;
- **Legal, audit & compliance**: Managing risk and anti-money laundering purposes ; Preventing irregularities and fraud; Contract management; Litigations; Whistleblowing;
- **Security & IT**: IT system administration and management, monitoring the use of digital equipment/devices and digital traffic; security events investigation; monitoring and recording of Internet usage history and e-mail correspondence
- **Business operations**: business partners administration; management of business partners projects

Special focus on:

Processing personal data for fighting against financial crime

As part of our legal obligations to prevent money laundering and ensure compliance with international sanctions regulation and counter-terrorism financing risks, Europ Assistance may use and analyze Data subjects' personal data to establish profile and to determine the risks of money laundering in accordance with the criteria of the French Monetary and Financial Code and/or the counter-terrorism financing risks in accordance with European Union regulations.

Processing personal data for fighting against fraud and irregularities purposes

When filing a claim, the Data Subjects' personal data may also be used to combat insurance fraud, e.g. the fraudulent exaggeration of claims, fake claims, checking identity.... The fight against fraud is carried out in the legitimate interest of Europ Assistance, but also for the protection of the insured community. In the event of proven fraud, Europ Assistance may initiate criminal proceedings and implement relevant measures to protect its interests and the interests of its customers.

Recipients

EA Legal Entities may share/disclose Data subjects' personal data with the following recipients:

- relevant services of EA Legal Entities and/or Generali Group companies;
- reinsurers and brokers;
- third parties engaged by EA and performing services on our behalf (e.g. IT suppliers, subcontractors and freelancers);
- certain regulated professionals (e.g. banks, lawyers, notaries and auditors);
- administrative, judicial or governmental authorities, state agencies or public bodies, strictly in accordance with Applicable Data Protection Legislation.
- Business partners

APPENDIX 2: EA LEGAL ENTITIES PROCESSING ACTIVITIES AS A DATA PROCESSOR

Data subjects concerned

As part of day-to-day business operations acting as a Data Processor, EA Legal Entities may collect and process Personal Data relating to:

- Policyholders
- Beneficiaries and insured
- Clients and prospects,
- Any other third party.

Personal data processed

Depending on the interaction EA Legal Entities may have with the Data subjects listed above, EA may collect and/or process the following categories of personal data:

- Identity and contact information (e.g., name, date of birth, gender, address, passport)
- Demographic data & Personal life data
- Professional life data (e.g., job title & company)
- Economic and financial data (e.g., bank account, credit card number)
- Data related to geolocation and movements (e.g., data extracted from black boxes, GPS),
- Any data which may be relevant to provide assistance (including medical and health data)
- Any relevant data provided to EA in the contact forms /help center

Personal data processing activities

EA Legal Entities may process Data subjects' personal data for the following purposes:

- **Travel assistance services:** travelers support, assistance & repatriation;
- **Road assistance services:** roadside assistance;
- **Concierge services**: manage customers requests & business partnerships
- **Home & family assistance:** teleassistance; handle emergency interventions, protect homes, deliver personalized care and assistance to families; Identity theft protection

Recipients

EA Legal Entities may share/disclose Data subjects' personal data with the following recipients:

- Business partners
- Relevant services of EA Legal Entities and/or Generali Group companies;
- Third parties engaged by EA and performing services on our behalf (subprocessors);
- Administrative, judicial or governmental authorities, state agencies or public bodies, strictly in accordance with Applicable Data Protection Legislation.