ACE
BY FPG AIM

expandwithace.com

GENERAL DATA PROTECTION PROCESSING

Document Owner	GDPO
Date Created	18 July 2023
Date Modified	
Classification	FINAL
Version	1.1
Review History	

CONTENTS

1. Introduction
- General provisions
- Subject matter and objectives
- Definitions

2. Principles relating to processing of personal data
- Lawful, fair, and transparent
- Limited for its purpose
- Data minimization
- Accurate
- Retention
- Integrity and confidentiality
- Conditions for consent
- Processing of special categories of personal data

3. Rights of the data subject
- Exercise of the data subject
- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to object

4. Controller and processor
- Responsibility of the controller
- Data protection by design and by default
- Joint controllers
- Processor
- Record of processing activities
- Security of processing
- Notification of a personal data breach to the supervisory authority
- Communication of a personal data breach to the data subject
- Data protection impact assessment
- Designation of the data protection officer
- Position of the data protection officer
- Tasks of the data protection officer
- Monitoring, audit, and training

5. Transfer of personal data

- General principle for transfers
- Transfers on the basis of an adequacy decision
- Transfer of disclosures

6. Employees' Duties

1. Introduction

- General provisions

ACE is committed to being internationally compliant with Personal Data Protection Laws and regulations and to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all our legal obligations.

- Subject matter and objectives

ACE hold Personal Data about employees, clients, suppliers, and other individuals for a variety of business purposes.

This Data Protection Policy (the "Policy") sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy applies to all ACE offices, subsidiaries, and affiliates worldwide and requires staff to ensure that the General Data Protection Officer (GDPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The GDPO is an internal independent individual that is charged with ensuring that the personal data of the employees, clients, suppliers, or anyone else is processed in compliance with national and international data protection regulations, including but not limited to the European General Data Protection Regulation (Regulation (EU) 2016/679 of the European parliament and of the Council of 27th of April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "GDPR"). The GDPO is responsible for the implementation of necessary policies, processes, and controls to protect the privacy of all individuals involved in the organization's data processing and is responsible for monitoring ACE's compliance therewith.

Any data subject may approach the GDPO or any local data protection coordinator at any time to raise concerns, ask for or provide information on any observed data breaches as well as breaches or non-compliance of this Policy.

Contact details of the GDPO are as follows:

Email: dpo@expandwithace.com
Address: Av. Diagonal 453bis, planta 1, 08038 Barcelona, Spain

This policy is created to state the primary objective of ACE towards personal data processing. It describes the adequate level of the data protection amongst cross-border offices, subsidiaries, affiliates, and third parties, including those jurisdictions where legislation relating to the data protection is not yet adopted. All commitments listed in this Policy are described in a particular manner and covered in separate processes or additional specified policies prepared and approved by ACE.

- Definitions

ACE	ACE Group which shall include their worldwide affiliates and subsidiaries;
Binding Corporate Rules	Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
Consent	Of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
Controller (Data Controller/Data Joint Controller)	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing;
COO	Chief Operation Officer;
Cross-border Processing	Means either: (a) processing of personal data which takes place in the context of the activities of establishments; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in a particular jurisdiction which could be within the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member Stat;.
Data Subject	Any identified or identifiable natural person to whom Personal Data relate;
Enterprise	A natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
GDPR	The General Data Protection Regulation;
GDPO	The Group Data Protection Officer and person responsible for GDPR internally in ACE;
Filling Systems	Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
Identifiable Natural Person	Identifiable Natural Person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Main Establishment	(a) as regards a controller with establishments in more than one jurisdiction or Member State, the place of its central administration

	in that particular jurisdiction or in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in a particular jurisdiction or in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; (b) as regards a processor with establishments could be in more than one jurisdiction or in more than one Member State, the place of its central administration in a particular jurisdiction and in the Union, or, if the processor has no central administration in that particular jurisdiction or in the Union, the establishment of the processor in that particular jurisdiction or in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
Personal Data:	Any information relating to an identified or identifiable natural person (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;
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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Recipient	A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;
Representative	A natural or legal person established in a particular jurisdiction or in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
Restriction of Processing	The marking of stored personal data with the aim of limiting their processing in the future;
Special Categories of Personal Data	Personal Data, that is considered sensitive and is subject to specific Processing conditions, is: - Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; - Trade-union membership;

	- Genetic data, biometric data processed solely to identify a human being; - Health related data; - Data concerning a person's sex life or sexual orientation.
Supervisory Authority	Supervisory Authority Concerned: means a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority;
The Policy	Refers to ACE's Data Protection Policy;
Third Country	Third Country is not defined in the GDPR but ACE assumes it continues to mean any country or territory outside the European Economic Area;
Third Party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

2. Principles relating to processing of personal data

- Lawful, fair, and transparent:

Data collection and processing must be done lawfully, fairly and in a transparent manner in relation to the data subject.

- Limited for its purpose:

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

- Data minimization:

Any data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate:

The data hold must be 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.

- Retention:

ACE will not keep data for 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. ACE must take all necessary steps in order to safeguard the rights and freedoms of the data subject.

- Integrity and confidentiality:

The data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Other jurisdictions where ACE has an office may maintain or introduce more specific provisions to adapt the application of the rules of this Policy with regard to processing for compliance with above points.

This Policy comprises the internationally accepted data privacy principles without replacing the existing local laws. The relevant local law will take precedence in the event of a conflict with this Policy or when the local law has stricter rules than this Policy. The reporting requirements of data processing under local laws must be observed.

If there is a reasonable doubt that this Policy may contradicted with local legal requirements, the GDPO will work closely together with the relevant office to determine the best solution to meet the objectives of this Policy without breaching local laws.

- Conditions for consent

I. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
II. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
III. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
IV. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

- Processing of special categories of personal data

I. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

II. ACE collects and processes Personal Data of customers, business partners, and other third parties as much as is absolutely necessary for the establishment, execution and termination of any contractual relationship.

III. ACE also collects Personal Data for processing in cases of legitimate interest that may not necessarily requires the consent of the Data Subject. An example of legitimate interest will be the Due Diligence, Special Purpose Test required for Compliance reasons. In addition to this, in the case of a collectable debt, ACE can provide information to a Third Party Collector Agent for collection purposes.

IV. Within the employment relation, Personal Data which is absolutely necessary for the initiation, execution, and termination of the employment relation, may be processed. In case of the pre-employment, certain Personal Data may be collected, but if the employment relation does not start, any personal data protection collected must be erased.

3. Rights of the data subject

- Exercise of the data subject:

Individuals have rights to their data which we must respect and comply with to the best of our ability. ACE must ensure individuals can exercise their rights in the following ways:

- Right to be informed:

The controller shall take appropriate measures to provide any information to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The controller shall provide information on action taken on a request to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means

where possible, unless otherwise requested by the data subject.

Information provided as well of any communication in relation with the provision of information may be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Without prejudice to the obligation of providing information, where the controller has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

- Right of Access:

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with access to their personal data and supplementary information.

- Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

- Right to erasure

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay when there are no compelling reasons for continuing processing it.

- Right to restriction of processing

ACE must comply with any request to restrict, block, or otherwise suppress the processing of personal data.

ACE is permitted to store personal data if it has been restricted, but not process it further. ACE must retain enough data to ensure the right to restriction is respected in the future.

- Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing.

4. Controller and processor

- Responsibility of the controller

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

- Data protection by design and by default

The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures in an effective manner and to integrate the necessary safeguards into the processing in order to protect the rights of data subjects.

That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

- Joint controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their obligations.

- Processor

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Policy and ensure the protection of the rights of the data subject.

The processor shall not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Processing by a processor shall be governed by a contract or other legal act, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

- Record of processing activities

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
(e) where applicable, transfers of personal data to a third country or an international organization, shall include the identification of that third country or international organization;
(f) where possible, the envisaged time limits for erasure of the different categories of data;

- Security of processing

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

- Notification of a personal data breach to the supervisory authority

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification referred to above shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

- Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures.

The communication to the data subject shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

- Data protection impact assessment

Where 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 natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

The controller shall seek the advice of the GDPO, where designated, when carrying out a data protection impact assessment.

The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

- Designation of the data protection officer

The controller and the processor shall designate a data protection officer who shall be designated on the basis of professional qualities and, in particular, knowledge of data protection law and practices and the ability to fulfil his/her tasks il the tasks.

The controller or the processor shall publish the contact details of the data protection officer.

- Position of the data protection officer

The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
.
The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his/her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data.

The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks.

- Tasks of the data protection officer

The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the general data protection provisions;

(b) to monitor compliance with this policy in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance.
(d) the data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

- Monitoring, audits, and training:

I. Monitoring: All employees must acknowledge this policy. The GDPO has overall responsibility for this policy. ACE will keep this policy under review and amend or change it as required.
II. Audits: Regular data audits to manage and mitigate risks will have to be conducted at regular basis.
III. Training: All employees must receive training specific for their role. If the employee changes role, new data protection training relevant to the new role and responsibilities must be provided.

5. Transfer of personal data

- General principle for transfers

When Personal Data processed by ACE is to be transmitted to third parties or between ACE's offices, the data recipient is authorized to use the data strictly only for the defined purpose. Third parties must be compliant with data privacy requirements and ACE being the remitter of the data must ensure that it applies sufficient efforts to check the third parties' data protection policy.

If data is transmitted to a third party outside the European Union, especially to those countries where data privacy laws are yet not adopted, the recipient must agree to maintain transmitted data protection levels equivalent to this Data Protection Policy. For this purpose, the third party must sign a specific agreement with ACE.

In the event where Personal Data is transmitted from an ACE office establishes in the European Union to an ACE office in a third country, the recipient office is obliged to cooperate with the relevant Supervisory Authority within the European Union which supervises data protection implementation by ACE. Should there be a data breach in the event of such transmittal, the remitting office takes full responsibility to handle and report the data breach as it would have occurred within the European Union.

- Transfers on the basis of an adequacy decision

A transfer of personal data to a third country or an international organization may take place following an adequate level of protection, safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

- Transfer of disclosures

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the countries.

6. Employees' Duties

Every employee has the following duties with regard to the processing of personal data:

(a) Familiarizing with internal procedures and legal requirements with regard to data protection and compliance with these procedures and requirements;
(b) Liaising with the GDPO in case of uncertainties with regard to applicable data protection requirements;
(c) Notifying the GDPO of potential data breaches;
(d) Informing and forwarding GDPO the Data Subjects' access requests received during the performance of their duties and which have not been submitted to the proper e-mail inbox dpo@expandwwithace.com