PRIVACY POLICY

EU Reg. 2016/679

Abaco s.p.a.

Head Office

Piazza Vilfredo Pareto 9
46100 Mantova

Version 6

Revision	Publication date	Author	Reason for revision
0	22/05/2018	G.Ghilardi	First draft
1	12/02/2020	G.Ghilardi	Organigram Revision
2	31/03/2021	G.Ghilardi	Introduction Protocol 231. Expanding the scope of integrated management systems to SaaS services
3	16/11/2021	G.Ghilardi	Underlined parts Integration of ISO27017 and ISO27018 guidelines
4	22/4/2022	G.Ghilardi	Better specified UK branch integration ABACOGROUP Uk
5	24/05/2023	G.Ghilardi	Separate Abaco UK LTD Policy created, references in this policy removed.
6	21/05/2024	G.Ghilardi	Inserted DPO role

INDEX

1. PURPOSE AND SCOPE

The purpose of this document is to certify *Abaco .*'s position of compliance with the obligations introduced by **European Regulation 2016/679 on the** protection of individuals with regard to the processing of personal data and on the free movement of such data.

The privacy policies set out below apply to the processing of personal data of third parties for which *Abaco .* is the Data Controller, as defined by European Regulation 2016/679.

The policy applies to all Abaco Spa offices. Abaco UK LTD as a separate legal entity has created a separate Privacy Policy which follows the UK law "UK GDPR". At the moment and until otherwise agreed, the United Kingdom is equated with European countries by European community directive.

2. DEFINITIONS

For the purposes of this document:

(1) '**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference in particular to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity;

2) '**processing**' means 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;

3) '**restriction of processing**' means the marking of personal data stored with the aim of limiting their processing in the future;

(4) '**profiling**' means any form of automated processing of personal data consisting of the use of such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects of that person's professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) '**pseudonymisation**' means the processing of personal data in such a way that personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and subject to technical and organisational measures to ensure that such personal data is not attributed to an identified or identifiable natural person;

(6) '**controller**' means 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 are determined by Union or Member State law, the controller or the specific criteria applicable to its designation may be established by Union or Member State law;

7) '**controller**' shall mean the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

consent of the data subject' shall mean any freely given, specific, informed and unambiguous indication of the data subject's wishes, whereby the data subject, by a statement or an unambiguous affirmative action, indicates his/her agreement to personal data relating to him/her being processed.

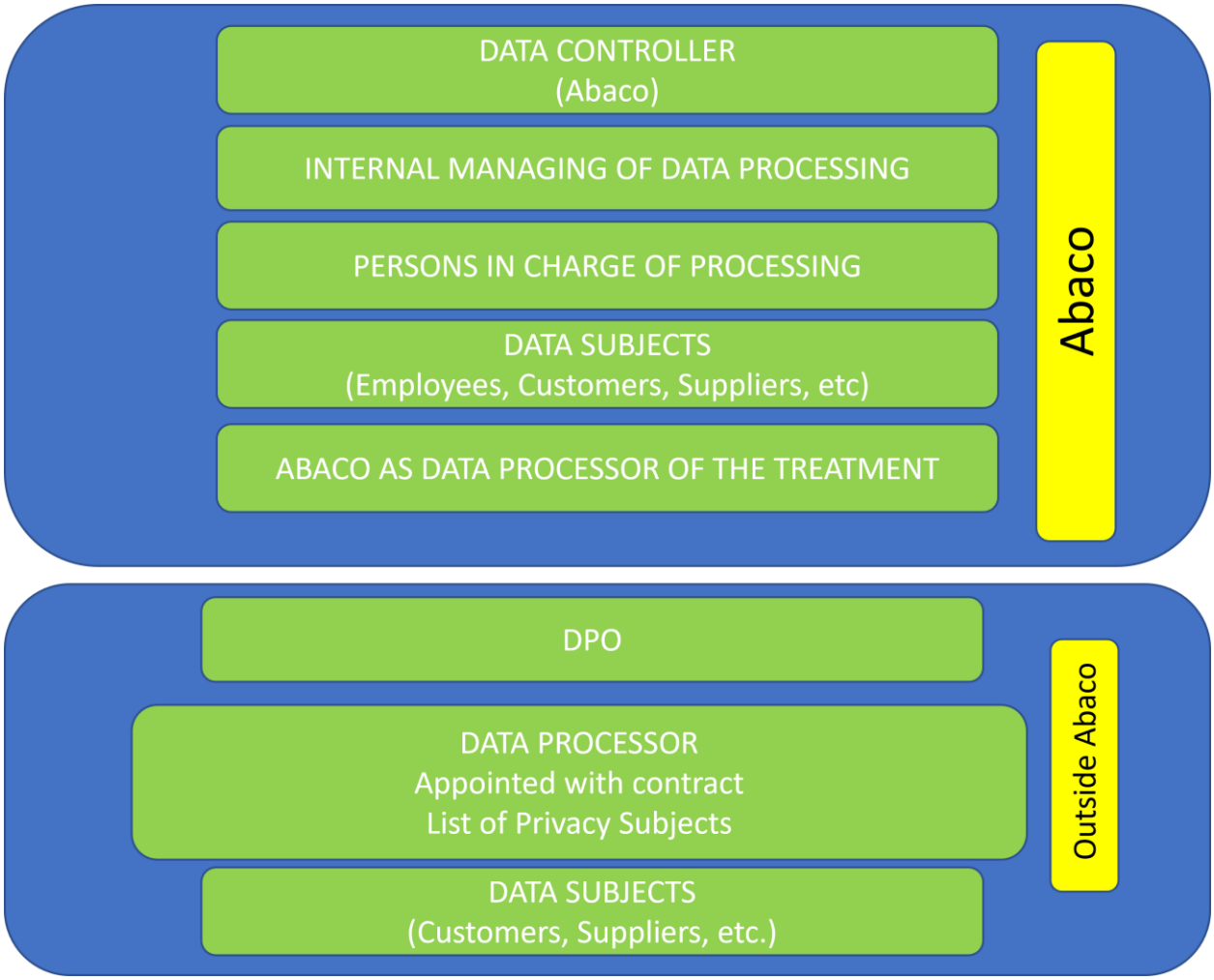
3. MODALITIES OF PERSONAL DATA PROCESSING

Abaco processes the personal data of third parties in accordance with the following principles:

a) treated in a lawful, fair and transparent manner vis-à-vis
b) collected for specified, explicit and legitimate purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; taking all reasonable steps to delete or rectify in a timely manner data that are inaccurate in relation to the purposes for which they are processed ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than the purposes for which they are processed ('limitation of storage');
f) processed in such a way as to ensure adequate security of personal data, including protection, by appropriate technical and organisational measures, against unauthorised or unlawful processing and accidental loss, destruction or damage ('integrity and confidentiality').

4. FIGURES INVOLVED IN DATA PROCESSING

4.1 Corporate Privacy Organigram



4.2 Internal and external stakeholders

4.2.1 Data controller

Abaco is the controller of the processing of personal data of natural persons as defined by Art. 4 para. 7 of REG (EU) 2016/679.
The data controller shall implement appropriate technical and organisational measures to ensure, and be able to demonstrate, that the processing is carried out in accordance with EU Regulation 2016/679.

4.2.2 Abacus External Processor

Abaco, where necessary, may act as External Data Processor, pursuant to Article 28 of REG (EU) 2016/679, in the context of service contracts concluded with its customers.

Abaco as External Data Processor puts in place appropriate technical and organisational measures to ensure, and be able to demonstrate, that the processing is carried out in accordance with EU Regulation 2016/679.

4.2.3 External Processors

Abaco has identified 'data controllers' as those persons outside the company and its branches or offices who are responsible for:

- management of practices relating to the hiring of workers and the management of payroll and/or other employment consultancy services;
- management of tax/accounting practices
- cloud service and hosting providers
- management system providers with assistance
- suppliers of outsourced SW supply services or "Time & Material" type services
- Portal providers such as the Whistleblowing reporting portal
- External companies of the group (Abaco UK LTD)

With these third parties Abaco signs a contract for the processing of data in accordance with Article 28 of REG (EU) 2016/679.

According to the indicated contract, the 'data controllers' identified by Abaco are obliged to:

- take appropriate technical and organisational measures so that the processing of personal data of third parties, the categories of which are specified in the contract by Abaco, meets the requirements of the EU Regulation 2016/679 and ensures the protection of the rights of the data subjects in accordance with the applicable legislation;
- ensure that persons authorised to process personal data, the categories of which are specified in the contract by Abaco, have committed themselves to confidentiality or have an appropriate legal duty of confidentiality;
- take all measures required under Article 32 REG (EU) 2016/679;
- taking into account the nature of the processing, to assist ABACO with appropriate technical and organisational measures, insofar as this is possible, in order to comply with the obligation of the data controller to follow up on requests for the exercise of the data subject's rights under Chapter III of EU REG. 2016/679;
- assist ABACO in ensuring compliance with the obligations set out in Articles 32 to 36 of REG(EU) 2016/679, taking into account the nature of the processing and the information available to the controller;
- at the request of the Controller, delete or return all personal data, the categories of which are indicated above, after the provision of services relating to the processing has ended. In both cases, the Data Processor shall, at the request of the Controller, provide the Controller with a written declaration stating that no copy of the personal data and information of the data subjects exists at the Controller;
- make available to the data controller all the information necessary to demonstrate compliance with the obligations set out in Article 28 of EU Reg. 2016/679;
- promptly communicate to the Data Controller requests from data subjects, objections, inspections or requests from the Supervisory and Judicial Authorities, and any other relevant information in relation to the processing of personal data;

- select sub-processors from among persons whose experience, capacity and reliability provide sufficient guarantees to put in place appropriate technical and organisational measures so that the processing meets the requirements of the applicable legislation and ensures the protection of the rights of data subjects;
- enter into specific contracts, or other legal acts, with the sub-contractors by means of which the Controller describes their tasks analytically and requires those persons to comply with the same obligations, with reference to data protection regulations, imposed by the Controller on the Controller pursuant to the applicable legislation (Art. 28 para. 4 EU REG 2016/679);
- retain towards the Data Controller the entire responsibility for the fulfilment of the obligations of the sub-processors involved, as provided for by the legislation in force (Art. 28 paragraph 4 EU REG 2016/679).

By concluding the data processing assignment contracts pursuant to Article 28 of REG (EU) 2016/679, ABACO grants general written authorisation to the Data Processors to be able to use any additional data processors ("sub-processors") established within the European Union.

4.2.4 Compliance Office

In order to comply with the obligations laid down in EU Reg. 2016/679 Abaco has identified the company function of the "Compliance Office" as the internal reference point for the implementation of the requirements introduced by the European legislation for all Abaco offices and branches.
The main tasks and duties of the compliance office with regard to the processing of personal data of natural persons and the free movement of data are summarised below.

Duties and tasks:

- Identification of 'data controllers';
- Arrangement of data processing assignment contracts in accordance with Art. 28 of REG (EU) 2016/679 with data processors;
- Archiving of existing contracts with data controllers and management of related changes;
- Preparation and updating of the processing register;
- Provision of information to data subjects;
- Management of the activities to be undertaken to exercise the rights of data subjects;
- Managing the activities to be undertaken for personal data breach notification;
- Planning and organising staff training on privacy issues;
- Responsible for the ISO 27001 corporate management system integrated with the ISO27017 and ISO27018 guidelines, to which reference is made for the application of technical/organisational measures for the secure processing of personal data.

4.2.5 Authorised Processing

The EU Reg. 2016/679 does not explicitly mention the figure of the 'processor', which was instead provided for in the previous legislation Legislative Decree 196/2003 'Privacy Code'.
Abaco relies on using the nomenclature 'Authorised Processors' to identify those individuals, other than data controllers, who work on behalf of the company in all locations and who may process personal data of third parties in accordance with their covered company role.

Authorised processors are therefore

- company employees or collaborators;

It should be noted that such persons may also be 'data subjects'.
However, in their role as 'authorised processors' they are obliged to:

- process personal data of natural persons lawfully and fairly;
- process the personal data of natural persons for the purposes determined, functional, explicit and legitimate on the basis of the corporate role held and the relevant work tasks;
- take steps to ensure that the data processed is accurate and as up-to-date as possible;
- use the utmost discretion, both inside and outside the company, with regard to personal data of which one has knowledge, taking care to protect them, particularly in cases where
  the information relates to characteristic elements such as health, family status or aspects of economic, cultural or social identity;
- not disclose personal data of natural persons outside the company, except in cases where this is necessary for the performance of the tasks assigned;
- use only the tools and programmes provided or authorised by the company and only to perform the assigned tasks;
- be familiar with the contents of this document (Privacy Manual);
- apply, to the extent of its competence, the procedures laid down in the Information Security Management System - ISO 27001 certified.

Abaco has appointed, by management appointment (6.17 AUT MOD Internal Data Processing Authorisation), those authorised to process the data of Abaco and its employees/collaborators at all locations and branches, and undertakes to appoint data processing authorisations according to the duties held and the intended processing of personal data from the time of recruitment.

4.2.6 Data subjects

The interested party is:

- the natural person (identified or identifiable) to whom the personal data relates.

The categories of data subjects whose personal data Abaco processes are listed in the processing register, the management of which is described below.
The exercise of the rights of the interested parties is guaranteed by Abaco . in the manner set out in this document.

4.3 Non-mandatory figures

4.3.1 DPO (Data Protection Officer)

According to Article 37 of REG (EU) 2016/679, the Data Controller must designate a DPO in the event that:

- the processing is carried out by a public authority or a public body (with the exception of judicial authorities when exercising their judicial functions);
- where the core activities of the Controller and the Processor(s) consist of processing operations which, by their nature, scope and/or purposes, require the regular and systematic monitoring of data subjects on a large scale;

- where the main activities of the above-mentioned entities consist in large-scale processing of special categories of personal data (sensitive data, genetic data, biometric data, judicial data).

ABACO does not fall within the above-mentioned cases for which the figure of DPO is mandatory. Therefore, a Data Protection Officer was not identified.

ABACO does not fall into the cases indicated above for which the figure of the DPO is mandatory, but despite not having the obligation, in order to have greater control and an external third party that can act as a collector of problems inherent to data processing, it has decided to appoint the company Seprim Srl in the person of Andrea Parma as DPO, with official notification to the privacy guarantor. The DPO can be contacted at dpo-mantova@abacogroup.eu. The DPO conducts an annual audit to review processes and documents.

4.3.2 EU Representative

Abaco is not required to appoint an EU Representative as the company is based within the European Union.

4.3.3 Reference legislature of the UK office (ABACOGROUP UK)

Abaco considers ABACO UK LTD to be equivalent to the Italian offices in terms of personal data protection. This is also in light of the decision of the European Community of 28/6/2021 which following Brexit issues the adequacy provision with an end date of 2025. The protection and English legislation (General Data Protection Regulation (General Data Protection Regulation) is considered to be of an appropriate level. UK GDPR)).

5. TREATMENT REGISTER

In order to have an up-to-date picture of the processing operations carried out Abaco . has equipped itself with the register of processing operations referred to in Article 30 of EU Reg. 2016/679.
The compliance department is responsible for drawing up this register and keeping its contents constantly updated for all Abaco locations.
The register contains:

- Data on the data controller
- Stakeholder categories
- Category of personal data processed
- Details of personal data processed in relation to category
- Methods of collecting personal data
- Time limit for deletion of personal data
- Purpose of processing
- Recipients to whom personal data are disclosed (internal/external to the company)
- Transfer of personal data to third countries/international organisations
- Instruments involved in treatment
- Technical/organisational security measures

6. INFORMATION TO DATA SUBJECTS AND CONSENT TO PROCESSING

The information template prepared by Abaco and addressed to data subjects contains:

a) the identity and contact details of the data controller;
b) the purposes of the processing for which the personal data are intended and the legal basis of the processing;
c) any categories of recipients of personal data;
d) the controller's intention to transfer personal data to a third country or international organisation;
e) period of retention of personal data;
f) the rights of the data subject;
g) whether the provision of personal data is a legal or contractual obligation or a necessary requirement for the conclusion of a contract, and whether the data subject is under an obligation to provide the personal data, as well as the possible consequences of failure to provide such data.

The compliance department customises the information according to the category of data subjects to whom it is addressed.
In relation to Internet browsing and the use of Cookies while browsing the company's websites, the information and consents have been entrusted to a specialised external provider (Iubenda) that provides compliance with the latest guidelines of the Garante.
The control of disclosures for the web-based platforms developed by Abaco is managed by the compliance department in cooperation with the development team.
Details on how to handle all Privacy treatments are contained in the operating instructions IST 07.02.01 and IST 07.02.02.
Below are the main ways in which disclosures are made to parties interacting with Abaco.

6.1 Arrangements for the transmission of information to interested parties

a) Company employees and/or collaborators
The compliance department ensures that employee and collaborator information is kept up-to-date according to the changing environment and applicable regulations.
The HR department is entrusted with the delivery and archiving of the information signed by employees at the time of recruitment on the company's integrated system, together with the entire package of documentation provided on entry into the company. In addition, privacy training is also included in the initial courses.
In the case of integration of standard information, it is the compliance department that is responsible for integrating the texts and obtaining the integration of consent from all those concerned.

In the case of processing of personal data of dependent adult family members, the explicit consent of the person concerned is required by signing the information notice.

b) Customers/Suppliers (natural persons)

Abaco Spa's communications with its customers/suppliers which take place via email contain, like all Abaco email addresses, a link that takes you back to the Abacogroup website where the privacy information pursuant to art. . 13 of EU Reg. 2016/679.

As regards contacts that potential customers may request through the company website, the request form contains the link to the information notice and requires explicit consent, which is compulsory for the normal processing of data provided for information requests, while it is optional for inclusion in marketing campaigns.

It is the marketing department that is in charge of checking consents according to the communications it intends to make.

With regard to events, including online events such as webinars, there is a specific disclosure, which is also prepared by the compliance department and then sent to and processed by the marketing department.

The contractual regulations with customers and suppliers concerning each party's data processing obligations are set out in the contract and any specific annexes.

On this point, too, please refer to the operating instruction mentioned above.

c) Natural persons registering on company portals

The company portals, which involve the collection of personal data of natural persons, have a privacy statement published in accordance with Article 13 of EU Reg. 2016/679.

After the data subject has read the published information notice, he or she must give his or her explicit (double) consent to the processing of his or her data by ticking the corresponding icon.

Once consent has been given, the system sends an email to privacy@abacogroup.eu with the data entered by the person concerned.

The compliance office archives the e-mails received.

The same applies to services provided in Saas mode and to applications published on mobile device stores. On this point, too, please refer to the operating instructions IST 07.01 and IST 07.02.02

d) Cookies Policy

The company website presents a cookie policy that reflects the indications of the Garante, listing in full all the cookies used by the site, divided into technical and third-party, and giving the user the possibility of accepting or disabling these cookies when accessing the site for the first time or even subsequently.

The same method is also used on the Abaco Farmer website and within the applications developed by Abaco.

At the moment, in order to facilitate the task of the compliance department and the communications department that maintains the corporate website and Abaco Farmer, the management of the cookie policy has been outsourced to an external provider (Iubenda), which guarantees compliance with the Garante's directives.

It is the responsibility of the compliance office to check that the disclosures are up-to-date, to update the publications on the applications developed by Abaco.

7. EXERCISE OF DATA SUBJECTS' RIGHTS

The rights of data subjects under EU Reg. 2016/679 are as follows:

Art. 15 EU Reg. 2016/679
Right of access

1.The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data relating to him are being processed and, if so, to obtain access to the personal data and to the following information:

a) the purposes of the processing;
b) the categories of personal data in question;
c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular if they are recipients in third countries or international organisations;
d) where possible, the intended period of retention of personal data or, if this is not possible, the criteria used to determine that period;
e) the existence of the data subject's right to request from the controller the rectification or erasure of personal data or the restriction of the processing of personal data concerning him or her or to object to their processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the data are not collected from the data subject, all available information on their origin;
h) the existence of an automated decision-making process, including profiling as referred to in Article 22(1) and (4), and, at least in such cases, meaningful information on the logic used, as well as the importance of such processing for the data subject and the envisaged consequences thereof.

Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the existence of appropriate safeguards within the meaning of Article 46 relating to the transfer.

3.The data controller shall provide a copy of the personal data undergoing processing. In case of further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. If the data subject makes the request by electronic means, and unless otherwise specified by the data subject, the information shall be provided in a commonly used electronic format.

4. The right to obtain a copy referred to in paragraph 3 shall not infringe the rights and freedoms of others.

Art. 16 EU Reg. 2016/679
Right of rectification

The data subject shall have the right to obtain from the controller the rectification of inaccurate personal data concerning him/her without undue delay. Taking into account the purposes of the processing, the data subject has the right to obtain the integration of incomplete personal data, also by providing a supplementary declaration.

Art. 17 EU Reg. 2016/679
Right to erasure (right to be forgotten)

1.The data subject shall have the right to obtain from the controller the erasure of personal data concerning him/her without undue delay and the controller shall be obliged to erase the personal data without undue delay if one of the following grounds applies

a) personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws the consent on which the processing is based in accordance with Article 6(1)(a) or Article 9(2)(a) and if there is no other legal basis for the processing;
c) the data subject objects to the processing pursuant to Article 21(1) and there is no overriding legitimate ground for processing, or objects to the processing pursuant to Article 21(2);

d) personal data have been unlawfully processed;
e) personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the data controller is subject;
f) personal data were collected in connection with the provision of information society services as referred to in Article 8(1).

Where a data controller has disclosed personal data to the public and is obliged pursuant to paragraph 1 to erase them, the data controller shall, taking into account available technology and the costs of implementation, take reasonable steps, including technical measures, to inform data controllers who are processing personal data of the data subject's request to erase any link, copy or reproduction of his or her personal data.

Paragraphs 1 and 2 shall not apply to the extent that the processing is necessary:
a) for the exercise of the right to freedom of expression and information;
b) for compliance with a legal obligation to which the processing is subject under Union or Member State law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for reasons of public interest in the field of public health in accordance with Article 9(2)(h) and (i) and Article 9(3);
d) for archiving purposes in the public interest or for scientific or historical research or statistical purposes in accordance with Article 89(1), insofar as the right referred to in paragraph 1 is likely to render impossible or seriously jeopardise the attainment of the objectives of such processing; or
e) for the establishment, exercise or defence of a legal claim.

Art. 18 EU Reg. 2016/679
Right of restriction of processing

The data subject shall have the right to obtain from the controller the restriction of processing when one of the following cases occurs:
a) the data subject contests the accuracy of the personal data, for the period necessary for the controller to verify the accuracy of such personal data;
b) the processing is unlawful and the data subject objects to the deletion of the personal data and requests instead that their use be restricted;
c) although the data controller no longer needs them for the purposes of processing, the personal data are necessary for the establishment, exercise or defence of a legal claim;
d) the data subject has objected to the processing pursuant to Article 21(1), pending verification as to whether the data controller's legitimate reasons prevail over those of the data subject.

Where processing is restricted pursuant to paragraph 1, such personal data shall, except for storage, only be processed with the consent of the data subject or for the establishment, exercise or defence of legal claims or the protection of the rights of another natural or legal person or for reasons of substantial public interest of the Union or a Member State.

A data subject who has obtained a restriction of processing pursuant to paragraph 1 shall be informed by the controller before that restriction is lifted.

Art. 19 EU Reg. 2016/679
Obligation to notify in case of rectification or erasure of personal data or restriction of processing

The controller shall communicate to each recipient to whom the personal data have been transmitted any rectification or erasure or restriction of processing carried out pursuant to Article 16, Article 17(1) and Article 18, unless this proves impossible or involves a disproportionate effort. The controller shall inform the data subject of such recipients if the data subject so requests.

Art. 20 EU Reg. 2016/679
Right to data portability

1.The data subject shall have the right to receive in a structured, commonly used and machine-readable format personal data concerning him or her that have been provided to a data controller and shall have the right to have those data transmitted to another data controller without hindrance by the data controller to whom he or she has provided them if:

a) the processing is based on consent within the meaning of Article 6(1)(a) or Article 9(2)(a) or on a contract within the meaning of Article 6(1)(b);
b) the processing is carried out by automated means.

When exercising his or her data portability rights pursuant to paragraph 1, the data subject shall have the right to obtain the direct transmission of personal data from one controller to another, if technically feasible.

3.The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. This right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 4.The right referred to in paragraph 1 shall not affect the rights and freedoms of others.

Art. 21 EU Reg. 2016/679

Right of opposition

The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her pursuant to Article 6(1)(e) or (f), including profiling on the basis of those provisions. The controller shall refrain from further processing the personal data unless he can demonstrate compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2.Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning him/her carried out for such purposes, including profiling insofar as it is related to such direct marketing.

3.If the data subject objects to processing for direct marketing purposes, the personal data are no longer processed for those purposes.

4.The right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information at the latest at the time of the first communication with the data subject.

5.In the context of the use of information society services and without prejudice to Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using specific techniques.
6.Where personal data are processed for scientific or historical research purposes or for statistical purposes pursuant to Article 89(1), the data subject shall have the right to object, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her, except where the processing is necessary for the performance of a task carried out in the public interest.

Art. 22 EU Reg. 2016/679

Automated decision-making concerning natural persons, including profiling

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her in a similar way.

Paragraph 1 shall not apply in the event that the decision:

a) is necessary for the conclusion or performance of a contract between the data subject and a data controller;
b) is authorised by the law of the Union or of the Member State to which the data controller is subject, which also specifies appropriate measures to protect the rights, freedoms and legitimate interests of the data subject;
c) is based on the explicit consent of the person concerned.

In the cases referred to in paragraph *2*(a) and (c), the data controller shall implement appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, at least the right to obtain human intervention by the data controller, to express his or her point of view and to contest the decision.

The decisions referred to in paragraph 2 shall not be based on the special categories of personal data referred to in Article 9(1), unless Article 9(2)(a) or (g) applies and appropriate measures are in place to protect the rights, freedoms and legitimate interests of the data subject.

Given that *Abaco .* does not carry out profiling activities, the exercise of the rights of the interested parties is guaranteed in the following ways:

- The data subject is informed that he/she can exercise his/her rights by making a request to privacy@abacogroup.eu. This information can be found in the "information on the processing of personal data" that *Abaco .* sends to all interested parties.
- The compliance department, which reads the e-mail address privacy@abacogroup.eu, takes over the request to exercise the rights of the person concerned and proceeds to
  a) enter the type of request in the 'privacy rights request register', indicating the date of receipt, personal details of the person concerned, type of request, internal offices of competence and/or external addressees involved;
  b) take steps to coordinate internal activities preparatory to the fulfilment of the data subject's request;
  c) verify that the data subject's request has been correctly taken care of by all the internal offices of competence and/or external addressees involved;
  d) inform the person concerned that *Abaco . has taken* steps to ensure the exercise of the right of the person concerned by complying with the request received.

8. TECHNICAL/ORGANISATIONAL SECURITY MEASURES

The technical/organisational security measures implemented by *Abaco* guarantee an adequate level of security in the processing of personal data of natural persons.
These measures generally guarantee

a) pseudonymisation and encryption of personal data, where possible;
b) the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services on an ongoing basis;
c) the ability to promptly restore the availability of and access to personal data in the event of a physical or technical incident;
d) the possibility of regularly testing, verifying and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

Abaco holds ISO 27001 (information security management system) certification extended to ISO27017 and ISO27018.
The procedures for information security techniques also apply to the processing of personal data of natural persons.
Therefore, please refer to the Information Security Management System implemented by *Abaco for the* specific definition and application of the technical/organisational measures on privacy.

8.1 Deletion of personal data from the archives

The deletion of personal data from *Abaco*'s archives in cases where the legal deadlines and/or those laid down in the 'processing register' are exceeded, is carried out in the following manner:

a) *Paper archives*: once a year, the compliance office, in cooperation with the competent offices, marks the paper documentation that has exceeded the set storage limit and commissions a third party company to shred it.

b) *E-mails*: data processors must delete e-mails from their e-mail addresses that have exceeded the set storage limit, following the procedures of the e-mail browser used. The compliance office verifies on the spot that this deletion has been carried out.

c) *Computer files*: data processors must ensure that documents containing personal data of natural persons that have exceeded the prescribed retention limit are deleted from their computer files. The compliance office verifies on the spot that such deletion has been carried out.
For all documents in the company, once they are deemed no longer useful, they are manually disposed of in accordance with the environmental policy, including through the use of document shredding machines.

9. PERSONAL DATA BREACH NOTIFICATION

WHEREAS, depending on the personal data of natural persons being processed, in the event of a breach, one of the following hypotheses is unlikely to apply:

- physical damage
- discrimination
- identity theft or usurpation
- financial losses
- injury to reputation
- economic damage
- social damage
- loss of confidentiality of data protected by professional secrecy

The compliance department will analyse the breach that has occurred and check whether it poses a risk to the rights and freedoms of the natural persons concerned.
If one of the aforementioned scenarios is likely to occur as a result of the breach, the data controller will notify the competent supervisory authority (see procedure for notification of personal data breaches, Section 9.2), for all Abaco locations and branches.
Otherwise, the breach suffered will be documented in the manner set out below (see handling of personal data breaches, Section 9.1) but not notified to the competent authority.

9.1 Managing data breaches

In the event of a breach, the compliance department fills in the form 'register of customer complaints, internal non-compliance and personal data breaches', documenting:

- the date on which the violation was found
- by whom the violation was detected
- the description of the breach
- the level of seriousness of the breach (minor - no Privacy Guarantor notification required/ serious - Privacy Guarantor notification required)
- analysis of the causes that led to the violation
- solution adopted
- status, outcome, date of implementation of the solution adopted
- any corrective action that is deemed necessary for the non-repetition of the same type of violation suffered
- timeframe for implementation, commissioning, closure of corrective action

9.2 Procedure for Reporting Violations

Reference authority: Privacy Guarantor
The Data Controller, in the cases set out in Section 9 of this document, shall notify breaches as set out in EU Regulation 2016/679 within 72 hours of the occurrence.
The compliance office applies the procedure currently defined by the Privacy Guarantor for the notification of violations, therefore:

1) Within 24 hours of the breach, it shall provide the Privacy Guarantor with summary information in relation to the breach that has occurred, supplementing the communication at a later date. Such summary information shall enable the Authority to make an initial assessment of the extent of the breach and shall therefore include:

- the identification data of the data controller;
- a brief description of the violation;
- the indication of the date, even presumed, of the infringement and the time of its discovery;
- an indication of where the data breach took place;
- an indication of the nature and content of the data even if only presumably involved;
- a brief description of the data processing or storage systems involved, including their location.

For the notification, the format currently prepared by the Authority 'data breach notification template' available on the website of the Privacy Guarantor will be used.

2) Within 72 hours of the breach, the compliance office shall notify the Privacy Guarantor of the manner in which the breach has been remedied and the measures taken or planned to be taken to prevent further breaches of the same kind;

3) Within 72 hours of the breach, the compliance office will notify the person concerned:

- the nature of the breach
- the type of personal data involved

- any recommendations that the person concerned should implement to mitigate possible negative effects
- the measures taken or planned to be taken by the data controller to prevent further infringements

10. STAFF TRAINING AND INFORMATION

10.1 Training

Training of company staff on privacy issues and in particular on the revision of internal procedures for the transposition of EU Reg. 2016/679 is carried out following the company procedures of the ISO 9001:2015 management system on internal training.

10.2 Information

All company data processors have this document available, uploaded to internal channels and on the company website, which they must comply with when managing the personal data of third parties.

Furthermore, a privacy training which summarizes the company position with respect to the new European Regulation and illustrates the rights of the interested parties is sent to those in charge of processing, also covering the role of interested parties in the processing, as indicated in point 6.

All new hires are given an initial course on the new regulation and internal procedures regarding data protection, differentiated according to the role held.

11. RELATED DOCUMENTS

- data processing information templates
- model contract of appointment for data controllers
- treatment register
- register of requests for privacy rights
- register of customer complaints, internal non-compliance and data breaches
- company organigram
- 6.17 AUT MOD Internal Data Processing Authorisation