Accelya Data Privacy Policy

Date: 31 March 2019

accelya

Information Security Classification Level

Level	Definition	
Public	Information that may be broadly distributed without causing damage to the organization, its employees and stakeholders	✔
Internal	Information which can be distributed within the company	✔
Confidential	Sensitive information available within a group of people which must not be disclosed outside the organization without explicit permission of document owner	
Highly Confidential	Highly sensitive and critical information meant for a limited group which must not be disclosed outside the organization without explicit permission of document owner.	

Contents

1. Introduction

Accelya collects uses and discloses Personal Information in accordance with applicable data privacy laws and as stipulated in this Data Privacy Policy ("Policy"), which outlines the standards by which Accelya will collect and use Personal Information.

This Policy should be read together with Accelya's Human Resources Privacy Policy, which describes the manner in which Accelya processes Personal Information in connection with recruitment and employment.

In order to assist Accelya in its compliance with the requirements of data privacy laws, all members of staff must read and observe this Policy when processing Personal Information on behalf of any Accelya company.

2. Definitions

"Accelya" means all Accelya group companies under the common control of Canary Topco Limited.

"Data Controller" means the entity which determines the purposes and means of processing of Personal Information.

"Data Processor" means an entity which processes Personal Information on behalf of a Data Controller.

"Data Subject" means an individual who is the subject of Personal Information.

"Personal Information" means data which allows the identification of an individual person directly or indirectly from that data. Examples may include name, address, email, telephone number, customer ID, or tax ID.

"Sensitive Personal Information" means information about a person relating to race or ethnic origin, sexual life or sexual orientation, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, genetic or biometric data, or criminal offences or criminal proceedings.

"Third Party" means an actual or prospective customer, distributor, reseller, vendor, supplier, consultant, professional adviser, business partner or any other third party that does or may do business with Accelya.

3. Data Privacy Principles

The core data privacy principles below are the foundation of this Policy.

3.1 Lawfulness, Fairness and Transparency

Accelya shall process Personal Information fairly, and in accordance with this Policy and applicable laws.

3.2 Purpose Limitation

Accelya will ensure that Personal Information collected is for specified, explicit and legitimate purposes and only to the extent necessary to fulfil those purposes.

3.3 Data Minimisation

Accelya will ensure that Personal Information is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

3.4 Data Accuracy

Accelya will take all reasonable steps to ensure that Personal Information is accurate and complete and will rectify or erase any incorrect Personal Information without delay, having regard to the purposes for which the Personal Information is processed.

3.5 Data Retention

Accelya will only keep Personal Information for as long is necessary to fulfil the purpose(s) for which it was collected or to comply with local law.

3.6 Data Security

All Personal Information collected will be processed in a secure manner.

These principles are further explained and expanded in section 7 below.

4. Purposes of Processing

4.1 Purposes

Accelya collects Personal Information in order to perform its business functions and to provide and/or to source services to and/or from Third Parties.

The standard purposes for which Accelya collects and processes Personal Information include:

- The administration of orders and accounts;
- The provision of products and services;
- Business development;
- Marketing, advertising and public relations in connection with Accelya's business activities, goods or services;
- Customer relationship management including satisfaction surveys, customer claims and after sales service;
- The conduct of Accelya's business activities;
- Compliance with applicable law or regulation;
- Any other purpose which the Data Subject is informed of from time to time when conducting business with Accelya.

4.2 Data Controllers and Data Processors

Many of the obligations under data protection law apply primarily to Data Controllers. Data Controllers determine the purposes and means of processing Personal Information. Data Controllers may engage others to undertake data processing activities on their behalf. Those other parties are known in data protection law as Data Processors.

5. Types of Data Collected

The types of Personal Information Accelya collects and processes include:

- Identification data, such as first and last name, date and place of birth, nationality, client ID;
- Contact details, such as address, telephone number and email address;
- Professional details, such as job title, affiliated organization, data related to transactions involving goods and services, data relating to business projects;
- When permitted by law, national identifiers, such as tax ID, government identification number;
- Financial data, such as bank account number, bank details; and
- Details of air travel, including bookings, flights, personal preferences, and services received.

5.1 Accelya may also collect Personal Information, directly and by automated means, whenever a third party accesses Accelya's websites.

For more information on how Accelya collects Personal Information on its websites, please refer to Accelya's Web Privacy Statement on the www.accelya.com www.revenuemanagement.com www.anari.aero and www.gocatapult.com websites.

6. Sharing and Disclosure of Data

Accelya only allows access to Personal Information by those who require access to perform their job duties and to third parties who have a legitimate purpose for access to that information.

6.1 Group Entities

All Personal Information collected will be processed in a secure manner.

6.2 Vendors and Suppliers

All Personal Information collected will be processed in a secure manner.

6.3 Customers

Accelya acts as a Data Processor in respect of certain Personal Information on behalf of its airline and other customers. The Personal Information processed will be shared with the customer concerned and with any third parties as may be directed by the customer, who will be the Data Controller in respect of that Personal Information.

6.4 Law Enforcement Purposes

Accelya may need to make disclosures of Personal Information if requested or required by government authorities, such as law enforcement authorities, courts, or regulators, or otherwise to comply with the law. Accelya may also transfer Personal Information to a Third Party if it or any of its affiliates is involved in a corporate restructuring (e.g., a sale, merger, or other transfer of assets).

7. The Data Privacy Principles In Practice

The following measures are designed to address each of the data protection principles referred to in Section 3 above. They will apply principally where Accelya is the Data Controller of the Personal Information in question. However, even where Accelya is a Data Processor, it must bear these principles in mind as they govern the rights of Data Subjects

7.1 Lawfulness, Fairness and Transparency

This principle encompasses several elements:

a) Transparency and Fairness

Accelya must obtain Personal Information fairly and not mislead or deceive Data Subjects as to how their Personal Information will be used.

In particular, Data Subjects must be provided with all of the following (often in the form of a “privacy notice”) when their Personal Information is first processed by Accelya, unless the information is already in their possession, or the provision of that information is not required by the term of any contract or by applicable law:

i. The purposes of any data processing;

ii. the legal ground on which the processing is based (see section (b) below);

iii. if the processing is based on the Data Subject's consent, the fact that the Data Subject has the right to withdraw their consent at any time;

iv. if the processing is based on a "legitimate interest", what that legitimate interest is (see section (b));

v. the recipients or categories of recipients with whom Accelya shares Personal;

vi. if applicable, the fact that Personal Information will be transferred outside of the EEA; whether the destination country has been deemed by the European Commission to provide adequate protection for Personal Information; and if applicable the means that have been used to protect the Personal Information in the destination country (for example the model clauses approved by the European Commission) and how the Data Subject can obtain a copy of them;

vii. the time period for which the Personal Information will be kept, or if that is impossible to state definitively, the criteria which will be used to determine that time period;

viii. the fact that the Data Subject has rights to access, rectify, erase, restrict, and object to the processing of their Personal Information which is held by Accelya;

ix. the fact that the Data Subject may complain to a data protection authority about how their Personal Information is processed;

x. where Personal Information is collected directly from the Data Subject, whether responses to requests for Personal Information are voluntary or obligatory, and the consequences of refusing to provide obligatory responses to requests for Personal Information; and

xi. where Personal Information is not collected directly from the Data Subject, the source of the Personal Information (or, if this is not possible, at least general information about the source).

Where Personal Information is collected directly from the Data Subject, this information must be provided at the time of collection. Where it is collected from other sources, this information must be provided as soon as possible and at the latest:

i. one month after Accelya receives the Personal Information;

ii. at the time of first communication with the Data Subject; or

iii. at the time Accelya gives the Personal Information to anyone else

b) Lawfulness – establishing the legal ground for processing Personal Information

Most data protection laws set out certain conditions, at least one of which must be met by Accelya, in order for Personal Information to be regarded as lawfully processed. In the EU Accelya has to inform Data Subjects which of these legal grounds applies to the processing of their Personal Information.

Personal Information cannot be processed by Accelya unless:

i. the Data Subject has given his/her consent for their information to be processed for one or more specific purposes (although note that there are very strict standards for what counts as consent – please see further section (d) below); or

ii. the processing is necessary for legitimate interests pursued by Accelya or a Third Party, except where those interests are overridden by the rights or legitimate interests of the Data Subject; or

iii. the processing is necessary for the performance of a contract with the Data Subject, or for the conclusion or termination of a contract with that person; or

iv. the processing is necessary for compliance with any legal obligation arising under European Union or European Member State law; or

v. the processing is necessary to protect the vital interests of the Data Subject or a Third Party (note that this condition is only rarely applicable, usually in medical emergencies); or

vi. the processing is necessary for the performance of a task carried out in the public interest (note that the public interest is of a relevant EU Member State, and because Accelya companies are private companies it is unlikely that this legal basis would be commonly applicable to processing carried out for or on behalf of Accelya).

In practice, the legal ground for most data processing by Accelya will be the "legitimate interest" ground. Situations where Accelya will generally have a legitimate interest in processing Personal Information include:

i. Sharing Personal Information between staff working for Accelya where this is necessary for internal administrative purposes;

ii. Processing which is necessary in order to prevent fraud;

iii. Processing Personal Information for IT security purposes.

c) Legal ground for processing sensitive Personal Information

The collection of Sensitive Personal Information is treated more strictly under data protection laws. Where you are required to process any Sensitive Personal Information, you should be aware that in addition to compliance with one of the basic conditions specified above, one of the additional conditions set out below must also be met:

vii. the Data Subject has given his/her explicit consent for the data to be processed for one or more specific purposes; or

viii. in relation to Personal Information of employees, the processing is necessary to enable Accelya to exercise its rights or obligations in connection with employment (for example, processing health data for statutory sick pay purposes).

There are other possible grounds for the processing of Sensitive Personal Information which are set out in applicable data protection laws.

d) Consent

As explained above, consent is one legal ground on which Personal Information can be processed. However, EU data protection laws set out very strict standards for what constitutes consent. In order for consent to be valid:

ix. it must be **freely given** (i.e. the Data Subject must be free to say "no");

x. it must be **specific to particular purposes** (e.g. 'I am happy for you to use my email address to send me information about your services');

xi. it must be **informed** –so people must be aware of the implications of what they are consenting to; and

xii. people must be informed that they can **withdraw consent** before they give it, and it must be as **easy to withdraw consent** as to give consent.

If Accelya is relying on consent as a ground for processing it must be able to demonstrate that it has obtained it. However, in practice, consent is likely to be required only where the processing cannot be said to be necessary either for the legitimate interests pursued by Accelya, or for the purposes of a contract with the Data Subject.

7.2 Purpose Limitation

Personal Information must only be obtained and stored in accordance with the purposes specified in privacy notices, which may include (among many other matters):

i. Staff Administration (for example payroll, provision of benefits, performance reviews, training);
ii. Relations with individual customers and with contacts at corporate customers and suppliers;
iii. Advertising, Marketing & Public Relations; and
iv. Accounts & Records.

7.3 Data Minimisation

The Personal Information processed by Accelya must be adequate, relevant and not excessive for its legitimate business purposes. Methods of collecting Personal Information must:

i. **Be specific to the particular purpose** for which Accelya is collecting the information in question. For example, if Accelya asks its staff to fill out a feedback form to understand how it can improve its procedures, the form should not ask for information which is irrelevant for this purpose, e.g. details of employment offer which an individual may have received from other organisations.

ii. **Not collect Personal Information that is simply "nice to have"**, which is otherwise not necessary for the purpose for which the Data Subject has provided their details, or which is to be used for another purpose (e.g. marketing) about which the Data Subject has not been informed. For example, it would not be appropriate to keep details of a person's ethnicity on file (unless required for diversity monitoring), because Accelya does not need this information in order to carry out its business operations.

Personal Information should also not be held for longer than is necessary for the purposes for which it is used. See 'storage limitation' at section 7.5 below for further information on this.

7.4 Accuracy

Every member of staff should comply with all procedures put in place by Accelya to make sure that the Personal Information they process is kept accurate and up to date.

If any member of staff becomes aware that Personal Information processed by Accelya about its employees, clients, contractors, consultants, or any other individuals is inaccurate or out of date, the relevant Personal Information should be updated or removed if possible. Personal Information relating to employees is managed centrally by Accelya's HR team and any request to update or remove that Personal Information should be directed accordingly.

7.5 Storage Limitation

Accelya must not keep Personal Information for longer than is necessary having regard to the purposes for which it is being processed. Personal Information should generally be held only for as long as is necessary:

i. To fulfil a justified business reason;
ii. To defend potential legal proceedings; or
iii. To comply with law or any requirement of a governmental or regulatory body.

Further details are contained in Accelya's Data Retention Policy.

7.6 Security

The maintenance of appropriate security is a vital part of Accelya's obligations under data protection laws. Members of staff must comply with all measures taken by Accelya to protect against unauthorised use of or access to Personal Information processed by it, including in particular the provisions of Accelya's Information Security Policy.

If any member of staff thinks that there may have been an IT security breach, or that Personal Information may have been lost, damaged, or accessed without authorisation, Accelya may have a legal obligation to inform the authorities within 72 hours of becoming aware of it. Therefore, it is of paramount importance that the IT Department and senior management are informed of any actual or potential security breach immediately.

8. Security and Integrity of Data

8.1 Accelya maintains appropriate administrative, technical and physical safeguards designed to help maintain the security, confidentiality and integrity of Personal Information and to protect it against accidental or unlawful destruction, accidental loss, unauthorised alteration, disclosure or access, misuse, and any other unlawful form of processing of the Personal Information in its possession.

8.2 The maintenance of appropriate security is a vital part of Accelya's obligations under data protection laws. Members of staff must comply with all measures taken by Accelya to protect against unauthorised use of or access to Personal Information,[including in particular Accelya's Information Security Policy.

9. Data Transfers

Personal Information may be transferred, accessed and stored globally as may be necessary for the uses and disclosures described above. Where Accelya transfers Personal Information from the European Union to another country outside the European Economic Area in circumstances where the transfer is not considered by the European Commission to provide adequate protection for the Personal Information, then the transfer will normally be made on the basis of the model contracts for international transfers approved by the European Commission, which are available on the Commission’s website.

10. Data Privacy Rights

10.1 Under EU data protection legislation Data Subjects have a right to access and to obtain a copy of their Personal Information, and to request that it is updated or rectified where it is outdated or inaccurate. Where it is no longer needed, they can request that Personal Information they have submitted to Accelya is deleted.

10.2 In certain circumstances, Data Subjects may also have the right under data protection legislation to object to Accelya's use of their Personal Information, to restrict Accelya's use of their Personal Information, and to be given a copy of their Personal Information in a commonly-used format to be provided, at their discretion, to another company.

10.3 Where Accelya's processing of a Data Subject's Personal Information is at any stage based solely on the Data Subject's consent then under EU law that consent can withdraw at any time, but in most cases Accelya will be processing their Personal Information on another legal basis, most commonly the fact that Accelya has a legitimate interest in processing the Personal Information for the purposes of its business, and that interest is not outweighed by the privacy interests of the Data Subjects concerned.

10.4 In the EU Data Subjects may exercise their rights free of charge by making an appropriate request to Accelya. Requests should be sent by email to privacy@accelya.com Data Subjects also have the right to complain to their local data protection regulator.

11. Direct Marketing

Accelya may use some of the Personal Information it collects from Third Parties for marketing purposes. Marketing emails will always contain an opt-out option.

Alternatively, recipients may opt out of receiving marketing messages by contacting optout@accelya.com

12. Who To Contact

For any questions or comments in relation to this Policy or Accelya's privacy practices, please contact: privacy@accelya.com