Accelya Data Privacy Policy

Version 0.2

August 19th 2024

Revision History

Version	Date	Amendments	Author	Approver
0.1	12/10/2023	First version	Ainhoa Sanchez/Sylvie Hay	Nicola Golunska
0.2	19/08/2024	Review and template change.	Nicola Golunska	Robert Wilson

Security Classification

Select one	Level	Definition
○	**Public**	Information that may be broadly distributed without causing damage to the organization, employees and stakeholders.
◉	**Internal**	Information that 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.

Distribution

Name
All employees

Contents

accelya

1. Introduction

All Accelya group entities under the common control of Accelya Global Limited (all business unitscollectively or individually referred to as, 'Accelya', 'the Company' or 'Companies') handle a variety of information about individuals ('Personal Data'), including information about:

- Customers;
- Passengers;
- Ground handling Agents;
- General Sales Agents;
- Employees;
- Independent contractors;
- Service Providers; and
- Visitors to our websites.

This Personal Data may 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, PNR, ticket number including bookings, flights, personal preferences, and services received.

In collecting and processing this Personal Data, the Company is subject to legal requirements designed to protect the rights of the individual (each a 'Data Subject') and protect the confidentiality, integrity and availability of the Personal Data.

This Policy should be read together with Accelya's Employee Privacy Notice, which describes the manner in which Accelya processes Personal Data 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 Data on behalf of any Accelya company.

2. Purpose

The purpose of this Global Data Privacy Policy (this 'Policy') is to define the key principles of data privacy and the minimum global requirements for Accelya regarding the collection and processing of Personal Data.

3. Scope

1. In scope

This policy applies to:

a) All Accelya group companies (or entities) under the common control of Accelya Global Limited and all related functions and business units;

b) All employees and independent contractors from any entity within paragraph 3.1a); and

c) All Personal Data processed by any entity in scope of paragraph 3.1a) or 3.1b), regardless of format.

2. Out of scope

This Policy does not apply to any entity which is not included in Accelya's group consolidatedaccounts, or to any data that is not Personal Data.

4. Policy Statement

Accelya is committed to protecting the Personal Data it collects or receives. We fulfill our responsibilities under global regulations such as General Data Protection Regulations (“GDPR”) both as a controller of Personal Data and also processing Personal Data on behalf of our customers.

Personal Data is defined in the GDPR. Article 4(1) of the GDPR states that Personal Data means any information relating to an identified or identifiable natural person’.

Under the India Digital Personal Data Protection Act, Personal Data means ‘any data about anindividual who is identifiable by or in relation to such data’.

Californian Consumer Privacy Rights Act (“CPRA”) provides one of the most comprehensive and strictest data privacy laws in the US. CPRA defines Personal Data to mean ‘information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household’.

This Policy defines Personal Data as data which allows the identification of an individual persondirectly or indirectly from that data. Examples may include name, address, email, telephone number, customer ID, or tax ID.

4.1. Direct and Indirect Data

Direct (data which may directly identify an individual).

Identifying data is Personal Data that can be used to single out and act on a specific individualwithout the use of further information.

Examples may include: name, ticket number, employee ID, social security number.

Indirect (data which in combination with other information may identify an individual)

Indirect data is Personal Data that is not in and of itself identifying but could be linked to an individual. It doesn’t have direct identifiers like name and address, but because of the presenceof semi (or ‘quasi’) identifiers like date of birth or post code or zip code, it is still reasonably likely that it could be linked to an identifiable individual.

5. Definitions

In this Policy, the following terms have the meanings defined below:

'Accelya' means all Accelya group companies under the common control ofAccelya Global Limited.

'Data Controller' means the entity which determines the purposes and means ofprocessing of Personal Data.

'Data Processor' means an entity which processes Personal Data on behalf of aData Controller.

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

'Direct Identifier' Data which may directly identify an individual.

'Indirect Identifier' Data which in combination with other information may identifyan individual.

'Personal Data 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.

'Data processor' describes a service provider (for example sub contractor) who processes Personal Data on behalf of a data controller. A data processor may only process personal data according to the instructions of the customer. Accelya acts asa data processor on behalf of its customers.

'Special Category Personal Data' means information about a person relating to race orethnic 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 partythat does or may do business with Accelya.

6. Principles

The requirements set forth in this Policy are based upon the following internationally accepted data privacy principles. In addition to the detailed requirements in this Policy, Accelya's businessfunctions must follow these principles when processing Personal Data.

1. Personal Data must be processed in compliance with applicable legal, contractual and regulatory requirements.
2. Personal Data must only be processed for specified, explicit and legitimatepurposes.
3. Personal Data must be processed transparently.
4. Personal Data processed by the Company must be relevant and limited to what isnecessary in relation to the purposes for which it is processed.
5. Personal Data must be accurate and, where necessary, kept up to date.
6. Personal Data must be retained for no longer than necessary to fulfill the businesspurpose for which it was collected.
7. Personal Data must be processed and managed securely to protect itsconfidentiality, integrity and availability

7. Minimum Requirements

This Policy sets forth certain minimum requirements that each business function, (for example Human Resources or Technology) must comply with in the collection and processing of Personal Data. These minimum requirements are global in nature and are subject to any variations required by applicable data protection law.

7.1 Accountability & Governance	
7.1.1	Accelya Executive Committee ('Excom') members are accountable for the implementation and continual monitoring of compliance with this Policy.
7.1.2	Legal and Regulatory Requirements • All business functions must comply with applicable data protection laws for processing Personal Data. The relevant data protection law will take precedence in the event that it conflicts with this Policy or has stricter requirements than this Policy.
7.1.3	Employee Training • Each business function must ensure all employees and independent contractors with responsibilities related to Personal Data undertake training in data protection. Accelya's Privacy Team will organize relevant training for business functions to ensure our personnel are aware of their obligations. This training may include: a) Annual Data Protection training as required; and/or b) Specialist training as determined by Accelya's Group DPO.
7.1.4	Policy Compliance Assessment • Accelya's business functions will be assessed for compliance with this Policy, at least annually, and any non-compliance risks will be reported to the accountable Excom member.
7.2 Rights of Individuals	
7.2.1	Right to be Informed • Data Subjects must be informed about the collection and processing of their Personal Data. • Such information shall be provided: a) Prior to collecting the Personal Data;

	b) In Accelya's online privacy notice • As appropriate, such disclosures should describe: a) What types of Personal Data are collected; b) For what purposes it is collected and/or processed; c) What types of sources it is collected from; d) What types of third parties it is shared with or sold to; and e) The rights each Data Subject may possess and how to exercise them.
7.2.2	<u>Right to Access</u> • Applicable business functions may be required to provide the information required by the Privacy Team to respond to Data Subject requests to access their Personal Data or request information about themselves. • This may include: a) Specific Personal Data collected about the requesting Data Subject, subject to certain legal restrictions; b) Specific information about the purposes, sources, and recipients of the Data Subject's Personal Data; and c) General information about the Company's data practices. • Such information should be provided in a reasonably portable format.
7.2.3	<u>Right to Rectify</u> • Accelya must respond to a Data Subject's requests to rectify inaccurate Personal Data. Such responses will be managed by the Privacy Team. • In response, and if instructed by the Privacy Team, the applicable business function must correct the inaccurate information, cease processing the inaccurate information, or provide information to the Privacy Team to explain to the Data Subject why their Personal Data is accurate.
7.2.4	<u>Right to Object</u> • Accelya must respond to a Data Subject's objections to certain processing of their Personal Data.
7.2.5	<u>Right to Restrict Processing or Sharing</u> • Accelya must respond to a Data Subject's requests for certain processing activities to be restricted or ceased altogether. Such actions will be determined and managed by the Privacy Team in collaboration with the relevant business function.

7.2.6	Right to Deletion • Personal Data of Data Subjects who request deletion must, subject to certain legal restrictions, be deleted within the applicable period as required by the Privacy Team
7.2.7	Complaints • Accelya must inform Data Subjects how they can make a complaint or submit a request regarding their Personal Data and define a procedure to handle such complaints and requests. • Where required under applicable data protection laws, this procedure must include informing Data Subjects how to submit their complaint to the applicable data protection regulator.
7.2.8	Responding to Requests • Upon receipt of a request from a Data Subject relating to their Personal Data, Accelya must respond to the request without undue delay and, at the latest, within 28 days of receipt, or such other time period as required by applicable data protection Laws. The Privacy Team must be informed of all such requests and will manage the response to the Data Subject. • In exceptional cases, Accelya may refuse to comply with a request if it is manifestly unfounded, excessive or refusal is required to comply with other legal obligations. Any such decision will be made by the Privacy Team and Legal.
7.2.9	Records of Requests • Accelya will maintain records of all Data Subject requests received for at least 24 months.
7.3 Legal Basis and Transparent Processing	
7.3.1	Grounds for Processing and Purpose Limitation • All business functions must identify and document the specific purposes for which the Personal Data will be processed, before the processing takes place. This information must be shared with the Privacy Team. • Business functions must ensure that Personal Data is only processed for the specific purpose for which it was collected and is not further processed in any manner incompatible with such purpose(s).
7.3.2	Use of Consent • Where Accelya relies upon the consent of the Data Subject to process their Personal Data, the business function will ensure that records of consent are maintained.
7.4 Service Providers	

accelya

7.4.1	• Business functions must put in place a process to identify and record Service Providers and consult with Information Security and the Privacy Teams to assess the risk of such third-party processing activity.
7.4.2	• When a business function uses a Service Provider, the procuring manager must ensure the Service Provider complies with all due diligence requests and any risk remediation activities prior to onboarding. The privacy and Security teams will provide a list of appropriate technical and organisational measures to protect the Personal Data.
7.4.3	• When a business function uses a Service Provider, the procuring budget owner must ensure that the Service Provider is capable of timely and sufficiently responding to a Data Subject rights request, or reasonably assisting Accelya with such response.
7.4.4	• Where required by law, the business function must not engage a Service Provider unless there is a documented agreement between Accelya and the Service Provider incorporating at least the minimum requirements for Personal Data processing.
7.5 Providing Services to Third Parties	
7.5.1	• When Accelya contracts with a Third Party, including customers (for example airlines and industry bodies), to provide services, and such services involve Accelya's collection and/or processing of Personal Data, the contract must address Accelya's role in assisting the Third Party meet their data protection obligations.
7.5.2	• If the business function is handling Personal Data on behalf of and for the benefit of another company (for example a customer), it must immediately inform Accelya's Group DPO if it believes that their instruction to Process Personal Data infringes, or may infringe, on one or more applicable data protection laws or the requirements of this Policy.
7.5.3	• The business function must inform Third Parties with whom Personal Data has been shared of any modification, withdrawal or objections pertaining to the shared Personal Data, and implement appropriate policies, procedures and/or mechanisms to do so.
7.5.4	• The business function must ensure that there is a documented agreement between Accelya and the Third Party describing the minimum requirements for Personal Data processing before any Personal Data is shared.
7.5.5	• Business functions will ensure that Personal Data processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.
7.5.6	• Business functions will not use Personal Data processed under a contract for the purposes of marketing, advertising, research and development without establishing that the necessary rights have been obtained for such purpose from the applicable customer or Data Subject.
7.6 Record of Processing	
7.6.1	• Each business function is responsible for maintaining a 'Record of Processing' of Personal Data, also known as a 'Personal Data Inventory', including a description of transfers of data in scope of section 7.11.

accelya

	• Each Record of Processing shall have an owner responsible for its accuracy and completeness.
7.7 Data Accuracy	
7.7.1	• Business functions must implement processes to keep Personal Data accurate and, where necessary, up to date.
7.8 Data Retention	
7.8.1	• Business functions must ensure that Personal Data is not kept any longer than necessary and data retention periods are defined in a data retention schedule.
7.8.2	• Business functions must have documented procedures and mechanisms for the secure disposal of Personal Data at the end of the data retention period.
7.8.3	• A Third Party may determine the purpose(s) of processing and data retention requirements for Personal Data. A business function must return and/or securely dispose of the Personal Data in accordance with the applicable contract with such Third Party.
7.9 Security of Processing	
7.9.1	• Business functions must ensure appropriate risk based technical and organisational security controls (as defined by the Group CISO) are applied to protect against a loss of confidentiality, integrity or availability of the Personal Data.
7.10 Data Protection by Design and Privacy Risk	
7.10.1	• Business functions must identify, using a 'Data Protection Impact Assessment' (also known as a DPIA or privacy impact assessment), the potential risks associated with new processing activities or changes to existing processing activities, with a focus on processing activities involving Special Category Personal Data or financial data. All DPIA's must be approved by the Privacy Team.
7.10.2	• Applicable data protection laws and the controls set forth herein must be taken into account at the design phase of any processing activity or system.
7.10.3	• Privacy non-functional requirements ('NFRs') must be implemented throughout the full lifecycle of software development and implementation. Processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.
7.10.4	• Business functions must implement controls limiting the collection and processing of Personal Data (data minimisation) appropriate to the business unit's business purposes and the purposes for which the Personal Data was collected.
7.10.5	• Business functions must implement controls to limit the identification of individuals using privacy tools and techniques, aligned with the business unit's business purposes and the purposes for which the Personal Data was collected. For example, de-identification, tokenization and pseudo-anonymisation. Such controls must be aligned to standards as set out by Accelya's CISO.

accelya

7.10.6	• The Business function must either delete Personal Data or render it in a form which does not permit identification or re-identification of Data Subjects as soon as the Personal Data is no longer necessary for the identified purpose(s). Where such Personal Data is being processed on behalf of a Third Party, such deletion of de-identification must comply with any applicable contractual obligations.
7.10.7	• Personal Data must be transmitted (e.g. between systems or to a Third Party) using protocols with appropriate controls designed to ensure that the Personal Data reaches its intended destination.
7.11 International Data Transfers	
7.11.1	• Each business function must consult with the Legal and Privacy Teams to determine and ensure the appropriate safeguards required by applicable data protection laws are in place prior to the transfer of Personal Data from one country to another. • The business function must consult with the Legal and Privacy Teams to reasonably ensure that the international recipient entity is compliant with the data protection laws of the transferring entity.
7.12 Data Breach Management and Breach Notification	
7.12.1	• The Company must adhere to the Accelya Group process for data breach management. • The steps of this process include: a) The logging of all data breach events. b) Where required by applicable data protection laws, Accelya's Group DPO, alongside Legal and the CISO will determine the communication of data breach events to customers, partners, regulators and/or Data Subjects.
7.12.2	• Accelya must ensure that where required by applicable data protection laws, regulators are notified of a suspected data breach without undue delay but no later than 72 hours after its discovery, unless such data protection laws require otherwise.
7.12.3	• Accelya may be required to ensure that potentially impacted Data Subjects are notified of a suspected data breach. Where necessary, such notification should be made without undue delay but no later than 30 days after its discovery, or as otherwise directed by the applicable data protection laws.
7.12.4	• Accelya must retain a record of every data breach for at least 24 months.
7.13 Roles & Responsibilities	
7.13.1	• Accelya's Executive Committee ('Excom') are accountable for their business functions' compliance with this policy.
7.13.3	Accelya – Group DPO

accelya

	• Responsible for the development of this Policy and the Global Data Privacy Framework ('Framework') • Oversee Accelya's compliance with this Policy, the Framework and applicable data protection laws. • Advise business functions on how they can meet the requirements of this Policy, the Framework and applicable data protection laws.
7.13.4	Executive Committee ('Excom') • The Excom are responsible for ensuring that the appropriate data protection controls are designed, documented, implemented and monitored to meet the requirements of this Policy and the Framework in their area of responsibility. • Excom members also take on the role of 'Data Privacy Risk Owners' pertaining to the Personal Data as processed and owned within their business functions.
7.13.5	Business Process Owners ('BPOs') • Each business function must identify individuals who are accountable for each business unit's processing activities, (and record such individual in the Record of Processing). • The BPOs also take the role of 'Data Privacy Risk Managers' who are responsible for managing data privacy risk remediation activities related to their Records of Processing.
7.13.6	All Accelya Employees • All Accelya employees and contractors identified in Section 3.1 involved in the processing of Personal Data are responsible for protecting Personal Data and meeting the minimum requirements in this Policy.

8. Non-Compliance with this Policy

Compliance with this policy is mandatory for all Accelya Staff and any non-compliance identified with the Policy should be reported as quickly as possible totheir line manager, the Privacy or Legal Teams or Accelya's Group DPO.

If you have any questions, concerns or suspect non-compliance with this policy you should discuss this with the Privacy or Legal teams who will provide support as necessary.

Accelya Senior Management will conduct a fair and comprehensive investigation of any reported incidents or behaviour and will review the outcome of all reports and investigations and will ensure that appropriate and proportionate disciplinary action,up to and including termination, is taken in each.

9. Report a Data Breach

If any member of staff thinks that there may have been an IT security incident, or that Personal Data may have been lost, damaged, or accessed without authorisation, Accelya may have a legal obligation to inform regulators within 72 hours of becomingaware of it. Therefore, it is of paramount importance that the Information Security or the Privacy Team are informed of any actual or potential security breach immediately.

Information Security	Secops@accelya.com
Privacy Team	Privacy@accelya.com