air astana group	Data Privacy Policy	
	Department:	Compliance Service
	Number:	GRP-POL-CMP-Privacy_v3
	Effective date:	15.10.2026
	Number of pages	14
	Appendices:	1

DATA PRIVACY POLICY
of the Air Astana Group

air astana group	Data Privacy Policy	
	Department:	Compliance Service
	Number:	GRP-POL-CMP-Privacy_v3
	Effective date:	15.10.2026
	Number of pages	14
	Appendices:	1

Contents

1. Purpose and Scope 2
2. Key Terms and Definitions 2
3. Principles of Personal data Processing 4
4. Roles and Responsibilities 6
5. List of Personal data Necessary and Sufficient for the Performance of the Relevant Tasks 8
6. Legal bases for the Collection and Processing of Personal data 8
7. Collection and Processing of paper copies of identity documents 8
8. Third-Party Risk Management 8
9. Cross-Border Transfer of Personal data 9
10. Storage, Localisation and End of the Data Life Cycle 9
11. Data transfers for statistical, sociological, scientific and marketing research 10
12. Rights of Subjects and procedure for handling requests 10
13. Security Breaches and Incident Response 10
14. Liability 11
15. Change Management 11
16. References 11
17. Conflict-of-Laws Rule 12

Appendix 1. 14

	Data Privacy Policy	
air astana group	**Department:**	Compliance Service
	Number:	GRP-POL-CMP-Privacy_v3
	Effective date:	15.10.2026
	Number of pages	14
	Appendices:	1

1. Purpose and Scope

1. This Data Privacy Policy (the Policy) establishes uniform requirements of the Air Astana Group for the collection, processing, storage, use, transfer, protection, Deletion, Destruction, Depersonalisation and other handling of the Personal data of customers, passengers, employees, candidates, representatives of counterparties and other individuals.
2. The purposes of the Policy are to:
   - ensure compliance with the legislation of the Republic of Kazakhstan on Personal data and its protection;
   - protect the rights and legitimate interests of Personal data Subjects;
   - ensure the secure and justified use of Personal data in the Group's passenger, operational, employment, commercial, digital and other processes;
   - comply with applicable foreign legislation where such legislation applies to the Group's activities;
   - establish clear rules for employees and foster a culture of responsible handling of Personal data.
3. This Policy applies to the companies comprising the Group.
4. Group or Air Astana Group means Air Astana JSC, FlyArystan JSC, AATS LLP and any other legal entities in which Air Astana JSC directly or indirectly owns 50 (fifty) per cent or more of the shares or participating interests.
5. The Policy applies to Personal data processed by the Group in electronic, paper, audio, video or any other form, regardless of where the data are obtained, the system or medium used, or the citizenship or location of the Subject.
6. The Policy is mandatory for all employees who access Personal data on behalf of the Group.
7. The Policy is a framework document. Some of its provisions are further detailed in separate procedures, rules and other internal regulatory documents of the Group.

2. Key Terms and Definitions

8. For the purposes of this Policy, the following terms and definitions apply:
   1) **Business process owner** - the head of a structural unit or another designated employee of the Group whose area of responsibility includes a process involving the collection, processing, storage, use, transfer or Destruction of Personal data.
   2) **Collection of Personal data** - actions aimed at obtaining Personal data.
   3) **Compliance service** - a structural unit of Air Astana JSC that coordinates the requirements of this Policy, consults Business process owners, monitors compliance with privacy requirements and liaises with other units on Personal data matters.

4) **Database containing Personal data** - a structured collection of Personal data, regardless of the type of medium or digital object used.
5) **Deletion of Personal data** - removal of Personal data from a digital object or database without the possibility of recovery.
6) **Depersonalisation of Personal data** - actions that make it impossible to determine that Personal data relate to a particular Personal data Subject.
7) **Destruction of Personal data** - actions as a result of which Personal data cannot be restored.
8) **Digital object containing Personal data** - a digital object containing a structured collection of Personal data.
9) **Operator of a database and/or digital object containing Personal data** - a person/entity that collects, processes and protects Personal data.
10) **Owner of a database and/or digital object containing Personal data** - a person/entity exercising, in accordance with the laws of the Republic of Kazakhstan, the rights to possess, use and dispose of a paper-based database and/or digital object containing Personal data;
11) **Person responsible for organising Personal data Processing** - a person appointed by each individual Group company to organise internal compliance with Personal data Processing requirements in accordance with legislation and internal documents.
12) **Personal data** - information or a set of information about a Personal data Subject, supplemented by one or more Personal data Identifiers. Examples may include booking information and flight records, travel history, passenger preferences, information regarding special services provided to the passenger, loyalty programme data, salary information, health information, photographs, audio or video recordings, and other information relating to a Personal data Subject.
13) **Personal data Identifiers** - information that makes it possible to identify a Personal data Subject or to link separate data sets concerning that person into a body of information that makes it possible to identify that Subject. Examples may include, without limitation, a full name, contact information, Individual Identification Number (IIN), passport number or other identity document number, booking reference (PNR), frequent flyer membership number, account credentials, and other unique identifiers.
14) **Personal data Security Breach** - a breach of Personal data protection resulting in unlawful dissemination, alteration, destruction or deletion, unauthorised dissemination of Personal data transmitted, stored or otherwise processed, or unauthorised access to such data.
15) **Personal data Subject** - an individual to whom Personal data relate.

16) **Processing of Personal data** - actions aimed at the accumulation, storage, alteration, supplementation, use, dissemination, depersonalisation, blocking and destruction of Personal data.
17) **Publicly available Personal data** - Personal data to which access is unrestricted on a lawful basis and subject to the Subject's Consent, where such Consent is required.
18) **Restricted-access Personal data** - Personal data access to which is restricted by the legislation of the Republic of Kazakhstan or the Group's internal documents.
19) **Subject's Consent** - permission for the collection and Processing of Personal data, confirmed by the Subject or the Subject's legal representative and provided by a method and in a form that enable evidence of its receipt in accordance with legislation.

3. Principles of Personal data Processing

9. The Group collects, processes and protects Personal data in accordance with the principles expressly established by the legislation of the Republic of Kazakhstan. In view of the international nature of the Group's activities, additional principles apply where they are required by applicable foreign legislation or adopted by the Group as a higher standard of protection and do not conflict with the mandatory requirements of the legislation of the Republic of Kazakhstan.
10. The Collection, Processing and protection of Personal data within the Group are carried out in accordance with the following principles:
    1) **Respect for constitutional human and civil rights and freedoms.** Any action involving Personal data must take into account the individual's right to privacy, personal and family secrets, protection of honour and dignity, and other rights and freedoms. Processing must not create unjustified, disproportionate or discriminatory interference with the Subject's private life.
    2) **Lawfulness.** Personal data shall be collected and processed only with the Consent of the Subject or the Subject's legal representative, or where Processing without Consent is expressly permitted by legislation.
    3) **Specific, predetermined and lawful purposes.** Before the Collection and Processing of Personal data begins, a specific business purpose must be identified and documented. Personal data shall be used only for previously stated purposes. Use for a new purpose is permitted after assessing its compatibility with the original purpose, confirming a lawful basis, determining whether the Subject must be notified and, where required, obtaining new Consent.
    4) **Necessity and sufficiency.** The Group processes only Personal data that are objectively necessary and sufficient to perform the relevant task and are included in the "List of Personal data Necessary and Sufficient for the Performance of the Relevant Tasks".

5) **Reliability, accuracy and currency.** Structural divisions shall take reasonable measures to verify data according to the purpose for which they are used, enable correction and supplementation, and shall not use data known to be inaccurate or outdated when making decisions that may affect an individual's rights and interests.
6) **Storage limitation.** Personal data shall be retained no longer than required by the purposes of Processing, legislation, contractual obligations, claims-related obligations or other obligations of the Group. At the end of the established period, the data shall be Destroyed, Deleted, Depersonalised or otherwise transformed as provided by legislation.
7) **Access restriction and use solely for business purposes.** Access to Personal data shall be granted on a need-to-know basis and only to the extent required for a particular role. Accessing information about passengers, employees or other persons out of personal interest, at the request of acquaintances or for purposes unrelated to official duties is prohibited.
8) **Confidentiality of Restricted-access Personal data.** Employees who have access to Restricted-access Personal data may not disclose, disseminate, publish, forward or otherwise make such data available to persons without appropriate authorisation. The duty of confidentiality continues after the termination of employment, contractual or other relations with the Group.
9) **Transparency and awareness of the Subject.** In the cases and to the extent required by applicable legislation, the Subject shall be provided with clear information on the purposes and methods of Processing, the categories of data, possible recipients, retention periods or criteria, rights and contact channels. Relevant notices on the Collection and Processing of Personal data and Consent forms must not conceal material terms, mislead the Subject or compel the Subject to provide optional data.
10) **Documentation and demonstrability of compliance.** Structural divisions whose business processes involve the Collection and Processing of Personal data must be able to demonstrate what data they process, for which task and purpose, on what basis, in which system, to whom the data are provided, how they are protected and when they are deleted.s
11) **Protection throughout the life cycle.** Protective measures apply from the point of Collection until the final Deletion, Destruction or Depersonalisation of the data and cover receipt, entry, storage, viewing, alteration, export, transfer, archiving and other Processing activities. The category and volume of data, method of Processing, number of persons with access, use of external suppliers, cross-border transfer considerations and other risks shall be taken into account when selecting protection measures.

4. Roles and Responsibilities

4.1 General provisions

11. Ensuring compliance with this Policy and legislation, and managing Personal data risks, form part of the Group's overall corporate governance, risk management, compliance control and information security system.
12. Depending on the nature of a particular process and the requirements of applicable legislation, the Group may act as the Owner and/or Operator of a database Containing Personal data and, under applicable foreign legislation, as a controller, joint controller, processor or a party performing comparable functions.
13. Each business process involving the Collection and Processing of Personal data must have a designated Business process owner.

4.2 Compliance service / Person responsible for organising personal data processing

14. Each Group company shall appoint, by administrative order, a Person responsible for organising personal data processing in accordance with the requirements of the legislation of the Republic of Kazakhstan.
15. At Air Astana JSC, this person is appointed within the Compliance service.
16. The Compliance service / Person responsible for organising Personal data Processing performs coordination and oversight functions relating to compliance with this Policy and legislation and does not replace Business process owners, the Information Technology Department (including the Information security unit) or other participants in Processing activities with respect to the duties and responsibilities assigned to them by this Policy and legislation.

4.3 Business process owner

17. The Business process owner is responsible for ensuring that the Collection and Processing of Personal data within the relevant business process:
    - are carried out for a specific, predetermined and lawful purpose;
    - have an appropriate legal basis;
    - are limited to Personal data that are necessary and sufficient to perform the relevant task;
    - do not continue longer than necessary to achieve the purpose or comply with legal requirements;
    - are protected by appropriate organisational and technical measures;
    - comply with other Personal data requirements established by legislation and this Policy, which, where necessary, are further detailed by the Business process owner in

procedures, instructions or other internal regulatory documents governing the relevant business process.

4.4 Information Technology Department

18. The Information Technology Department, including the Information security unit, implements information security requirements relating to the Collection and Processing of Personal data, including:
    - protection of Personal data;
    - identification, authentication, multi-factor authentication and access management mechanisms;
    - logging of events and user actions;
    - encryption, cryptographic protection and security of transmission channels;
    - vulnerability management and monitoring the installation of security tool and software updates;
    - participation in investigations of Personal data Security breaches;
    - implementation of other relevant requirements of legislation and this Policy, as further detailed, where necessary, in procedures, instructions or other internal regulatory documents of the Information Technology Department.

4.5 Legal department

19. The Legal department provides legal support on:
    - interpretation of the legislation of the Republic of Kazakhstan and applicable foreign legislation concerning Personal data;
    - preparation of standard contracts and Personal data Processing agreements;
    - disclosure of Personal data in response to requests from law enforcement and judicial authorities;
    - handling pre-trial claims and litigation;
    - preparation of the Group's position in dealings with government authorities and legal support during inspections by the authorised body;
    - other relevant matters within the requirements of legislation and this Policy, as further detailed, where necessary, in procedures, instructions or other internal regulatory documents of the Legal department.

4.6 Group employees

20. Each Group employee must comply with legislation, this Policy and the procedures, instructions and other internal regulatory documents governing Personal data matters insofar as they relate to the employee's activities.

5. List of Personal data Necessary and Sufficient for the Performance of the Relevant Tasks

21. To determine the permissible scope of Personal data collected and processed as part of the Group's activities, Business process owners whose business processes involve the Collection and Processing of Personal data shall prepare and approve a List of Personal data Necessary and Sufficient for the Performance of the Relevant Tasks (the List).
22. Business process owners are responsible for the completeness, accuracy and currency of the information contained in the List.
23. The template of the List is set out in **Appendix 1 to this Policy.**

6. Legal bases for the Collection and Processing of Personal data

24. Personal data are Collected and Processed with the Consent of the Subject or the Subject's legal representative, except where Processing without Consent is expressly permitted by the legislation of the Republic of Kazakhstan. For processes subject to foreign legislation, the relevant legal basis shall additionally be determined.
25. Consent and related evidence of its receipt must be retained for the duration of Processing and for the period necessary to demonstrate compliance.

7. Collection and Processing of paper copies of identity documents

26. The Collection and Processing of paper copies of identity documents are prohibited, except where expressly provided for by legislation. When verifying identity, preference shall be given to inspecting the original document or a digital document presented through the e-government services of the Republic of Kazakhstan.

8. Third-Party Risk Management

27. Where a relationship with a third party involves the collection, receipt, transfer, provision of access to or other Processing of Personal data, the Business process owner shall ensure that the agreement includes provisions governing the Processing of Personal data in accordance with legislation and this Policy.
28. With respect to provisions relating to Personal data, the agreement shall be agreed with the Compliance service and, where necessary, with the information security unit regarding the applicable information security measures.

29. Where Personal data are transferred without an agreement, including to government authorities, aviation authorities or other authorised recipients, the Business process owner shall ensure that the applicable legal basis for the transfer is identified and documented and that the statutory requirements governing the transfer are observed.
30. A general confidentiality clause in an agreement does not replace specific provisions on the Processing of Personal data.

9. Cross-Border Transfer of Personal data

31. A Cross-Border Transfer of Personal data shall be carried out only where there is a legal basis provided by legislation and subject to the conditions and restrictions established by legislation.
32. Before carrying out a Cross-Border Transfer, the Business process owner shall identify:
    - the purpose and legal basis of the transfer;
    - the country to which the Personal data are transferred;
    - the recipient of the Personal data;
    - the categories of Subjects and the scope of Personal data transferred;
    - the applicable requirements and restrictions relating to the transfer.
33. Where required by legislation, the necessary Consents of Personal data Subjects shall be obtained and/or other statutory conditions shall be fulfilled before the Cross-Border Transfer is carried out.
34. Where a Cross-Border Transfer is carried out under contractual arrangements, the relevant agreement shall provide for the applicable requirements governing the Processing and protection of Personal data.
35. Where a Cross-Border Transfer is carried out without an agreement, including to foreign government authorities, aviation authorities or other authorised recipients, the transfer is permitted where there is an appropriate legal basis and the applicable statutory requirements are observed.

10. Storage, Localisation and End of the Data Life Cycle

36. Personal data in electronic information resources shall be stored in a Database located within the territory of the Republic of Kazakhstan.
37. Personal data shall be retained no longer than necessary to achieve the purposes of their Collection and Processing, unless a longer retention period is established by the legislation of the Republic of Kazakhstan or applicable foreign legislation, or is justified by another legitimate necessity.

38. The Business process owner is responsible for determining, documenting and observing the Personal data retention period within the relevant business process.
39. Upon expiry of the established retention period, Personal data shall be Deleted, Destroyed, Depersonalised or otherwise handled in a manner that prevents further identification of the Subject, unless continued retention is required on a lawful basis.

11. Data transfers for statistical, sociological, scientific and marketing research

40. When Personal data are transferred for statistical, sociological, scientific or marketing research, the data must first be Depersonalised, unless the transfer of information enabling Subjects to be identified is expressly provided for by legislation and has a separate appropriate legal basis.

12. Rights of Subjects and procedure for handling requests

41. The Group enables Personal data Subjects to exercise their rights in accordance with the legislation of the Republic of Kazakhstan and, where applicable, the requirements of foreign legislation.
42. A Personal data Subject's rights shall be fulfilled, or their fulfilment refused on lawful grounds provided by legislation, within the time limits established by legislation. Where necessary, the relevant detailed procedure shall be set out in the procedures, instructions or other internal regulatory documents of the responsible structural units.
43. A Subject may exercise their rights personally or through a legal representative. Where a representative submits a request, the Group may request documents confirming the representative's authority.

13. Security Breaches and Incident Response

44. An employee must immediately report any actual or suspected Personal data Security breach to the Compliance service (data.privacy@airastana.com) and the Information security unit (it.security@airastana.com).
45. Where an incident is related or potentially related to a Personal data Security Breach, the Information Technology Department investigates, contains and remediates the incident in accordance with the applicable internal regulatory documents of the Information Technology Department.
46. In the context of an actual or suspected Personal data Security Breach, the Compliance service, within its competence, ensures compliance with applicable Personal data legislation,

including considering whether the authorised body must be notified and, where such an obligation applies, arranging for the notification to be submitted within the statutory time limit.

47. The Compliance service and the Information Technology Department cooperate and exchange the necessary information where an incident is related or may potentially be related to a Personal data Security Breach.
48. The detailed procedure for registering, escalating, investigating, coordinating and documenting incidents is determined by the relevant internal regulatory documents of the designated structural units.

14. Liability

49. A breach of Personal data legislation and/or this Policy may result in disciplinary, administrative, civil or criminal liability in accordance with legislation and may also cause material and reputational harm to the Group.

15. Change Management

50. The Policy enters into force on the date of its approval by the Board of Directors of Air Astana JSC.
51. The Compliance service shall ensure that the Policy is reviewed at least once every three years and whenever there are material changes in legislation, business processes or the level of risk.
52. If any provision of the Policy becomes inapplicable due to a change in legislation, the remaining provisions shall remain in effect, and the relevant matter shall be governed by legislation until the Policy is amended.

16. References

53. The Policy has been developed on the basis of, and with due regard to, the following laws and regulations as in force at the date of approval of the Policy:
    - the Constitution of the Republic of Kazakhstan;
    - Law of the Republic of Kazakhstan dated 21 May 2013 No. 94-V "On Personal Data and Its protection";
    - Law of the Republic of Kazakhstan dated 24 June 2026 No. 326-VIII "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Digitalisation,

Personal data Protection, Road Traffic and Regulation of Advanced Technologies in Transport", insofar as its provisions apply from their respective effective dates;

- Rules for the Collection and Processing of Personal data, approved by Order No. 395/NQ of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 21 October 2020;
- Rules for Determining by an Owner and/or Operator the List of Personal data Necessary and Sufficient for the Performance of Their Tasks, approved by Order No. 199/NQ dated 21 June 2023;
- Rules for the Implementation by an Owner and/or Operator, and by a Third Party, of Measures to Protect Personal data, approved by Order No. 179/NQ dated 12 June 2023, as subsequently amended;
- Rules for Notification by an Owner and/or Operator of Personal data Subjects of a Personal data Security Breach, approved by Order No. 481/NQ dated 9 August 2024, as subsequently amended;

54. Given its activities in international markets, the Group also complies with international treaties ratified by the Republic of Kazakhstan and applicable foreign Personal data legislation where such legislation applies to the Group's activities. Such requirements may include Personal data protection legislation of the European Union, the United Kingdom, the People's Republic of China and other countries in which the Group operates.

17. Conflict-of-Laws Rule

55. In the event of a conflict between this Policy and applicable legislation, the requirements of legislation shall apply. Where the Policy establishes stricter requirements for privacy or the protection of Personal data, the stricter requirements shall apply.
56. The requirements of foreign legislation do not override the mandatory requirements of the legislation of the Republic of Kazakhstan. In the event of a potential conflict, the Compliance service (data.privacy@airastana.com) and the Legal Department (legal@airastana.com) must be consulted.

air astana group	Data Privacy Policy	
	Department:	Compliance Service
	Number:	GRP-POL-CMP-Privacy_v3
	Effective date:	15.10.2026
	Number of pages	14
	Appendices:	1

Revision History		
Revision number	**Changes (chapter number and title only)**	**Effective date**
v1	New document	08.09.2022
v2	RACI matrix added to Section II; Section X, Contact Information, added; Appendices 1 and 2 added; Sections V and VIII updated.	18.05.2023
v3	The Policy was revised and updated to reflect legislative changes. Its scope was extended to the Air Astana Group. New sections were introduced on the List of Personal data, legal bases for Processing, the prohibition on collecting paper copies of documents, localisation, retention periods and the end of the data life cycle. The RACI matrix was replaced with the "Roles and Responsibilities" section. Outdated provisions were removed and terminology was updated.	15.10.2026

Appendix 1.

List of Personal data Necessary and Sufficient for the Performance of the Relevant Tasks

No.	Description of the task, including functions, authorities and duties	Purposes of collection and processing within the task	Personal data required for the specified purpose	Documents or laws and regulations expressly providing for the tasks performed by the Owner and/or Operator