air astana group	Политика в области приватности данных	
	Департамент:	Служба комплаенс
	Номер:	GRP-POL-CMP-Privacy_v3
	Дата вступления в силу:	15.10.2026
	Количество страниц	16
	Приложения:	1

ПОЛИТИКА В ОБЛАСТИ ПРИВАТНОСТИ ДАННЫХ

Группы Эйр Астана

air astana group	Политика в области приватности данных	
	Департамент:	Служба комплаенс
	Номер:	GRP-POL-CMP-Privacy_v3
	Дата вступления в силу:	15.10.2026
	Количество страниц	16
	Приложения:	1

Содержание

1. Цель и область применения 2
2. Основные термины и определения 3
3. Принципы Обработки Персональных данных 5
4. Роли и обязанности 7
5. Перечень Персональных данных, необходимый и достаточный для выполнения осуществляемых задач 9
6. Основания для Сбора и Обработки Персональных данных 9
7. Сбор и Обработка копий документов, удостоверяющих личность, на бумажном носителе 10
8. Управление рисками третьих сторон 10
9. Трансграничная передача персональных данных 10
10. Хранение, локализация и завершение жизненного цикла 11
11. Передача данных для статистических, социологических, научных и маркетинговых исследований 12
12. Права Субъектов и порядок рассмотрения обращений 12
13. Нарушения безопасности и реагирование на инциденты 12
14. Ответственность 13
15. Управление изменениями 13
16. Ссылки 13
17. Правило разрешения противоречий 14

Приложение 1. 16

air astana group	Политика в области приватности данных	
	Департамент:	Служба комплаенс
	Номер:	GRP-POL-CMP-Privacy_v3
	Дата вступления в силу:	15.10.2026
	Количество страниц	16
	Приложения:	1

1. Цель и область применения

1. Настоящая Политика в области приватности данных (далее — Политика) определяет единые требования Группы Эйр Астана к сбору, обработке, хранению, использованию, передаче, защите, Удалению, Уничтожению, Обезличиванию и иному обращению с Персональными данными клиентов, пассажиров, работников, кандидатов, представителей контрагентов и иных физических лиц.
2. Целями Политики являются:
   - обеспечение соблюдения законодательства Республики Казахстан в сфере Персональных данных и их защиты;
   - защита прав и законных интересов Субъектов Персональных данных;
   - обеспечение безопасного и обоснованного использования Персональных данных в пассажирских, производственных, трудовых, коммерческих, цифровых и иных процессах Группы;
   - выполнение требований применимого иностранного законодательства в случаях, когда такое законодательство распространяется на деятельность Группы;
   - формирование понятных для работников правил и культуры ответственного обращения с Персональными данными.
3. Настоящая Политика распространяется на компании, входящие в Группу.
4. Группа или Группа Эйр Астана – означает АО «Эйр Астана», АО «FlyArystan», ТОО «AATS», а также любые иные юридические лица, в которых АО «Эйр Астана» прямо или косвенно владеет 50 (пятьюдесятью) и более процентами акций либо долей участия.
5. Политика распространяется на Персональные данные, обрабатываемые Группой в электронной, бумажной, аудио-, видео- или иной форме, независимо от места их получения, используемой системы, носителя, гражданства или места нахождения субъекта.
6. Политика обязательна для соблюдения всеми работниками, получающими доступ к Персональным данным от имени Группы.
7. Политика является рамочным документом. Некоторые ее положения конкретизируются отдельными процедурами, правилами и иными внутренними нормативными документами Группы.

2. Основные термины и определения

8. Для целей настоящей Политики используются следующие термины и определения:
   1) **База, содержащая Персональные данные** - совокупность упорядоченных Персональных данных, независимо от вида носителя и используемого цифрового объекта.
   2) **Владелец бизнес-процесса** - Руководитель структурного подразделения либо иной определенный работник Группы, в зоне ответственности которого находится процесс, предусматривающий сбор, обработку, хранение, использование, передачу или Уничтожение Персональных данных.
   3) **Идентификаторы Персональных данных** - информация, позволяющая идентифицировать субъект персональных данных или связать отдельные наборы данных о нем в совокупность сведений, позволяющих идентифицировать данного субъекта. К идентификаторам персональных данных могут относиться, помимо прочего, ФИО, контактные данные, ИИН, номер паспорта или иного документа, удостоверяющего личность, номер бронирования (PNR), номер участника программы лояльности, данные учётной записи и иные уникальные идентификаторы.
   4) **Лицо, ответственное за организацию Обработки Персональных данных** - назначенное каждой отдельной компанией Группы лицо, обеспечивающее организацию внутреннего соблюдения требований к Обработке Персональных данных в порядке, установленном законодательством и внутренними документами.
   5) **Нарушение безопасности Персональных данных** - нарушение защиты Персональных данных, повлекшее незаконное распространение, изменение и уничтожение и удаление, несанкционированное распространение передаваемых, хранимых или иным образом обрабатываемых Персональных данных или несанкционированный доступ к ним.
   6) **Обезличивание Персональных данных** - действия, в результате совершения которых определение принадлежности Персональных данных Субъекту Персональных данных невозможно.
   7) **Обработка Персональных данных** - действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение Персональных данных.

8) **Общедоступные Персональные данные** - Персональные данные, доступ к которым является свободным на законном основании и с учетом Согласия Субъекта, если такое Согласие требуется.
9) **Оператор базы и (или) цифрового объекта, содержащего персональные данные** - лицо, осуществляющее сбор, обработку и защиту Персональных данных.
10) **Персональные данные** - сведения или совокупность сведений о Субъекте Персональных данных, дополненные одним или несколькими Идентификаторами Персональных данных. Примеры могут включать сведения о бронированиях и совершённых перелётах, историю путешествий, предпочтения пассажира, сведения о специальных услугах, данные программы лояльности, сведения о заработной плате, сведения о состоянии здоровья, фотографии, аудио- и видеозаписи, а также иные сведения, относящиеся к субъекту персональных данных.
11) **Персональные данные ограниченного доступа** - Персональные данные, доступ к которым ограничен законодательством Республики Казахстан или внутренними документами Группы.
12) **Сбор Персональных данных** - действия, направленные на получение персональных данных.
13) **Служба комплаенс** - Структурное подразделение АО «Эйр Астана», координирующее требования настоящей Политики, консультирующее Владельцев бизнес-процессов, контролирующее выполнение требований приватности и взаимодействующая с иными подразделениями по вопросам Персональных данных.
14) **Собственник базы и (или) цифрового объекта, содержащего персональные данные** - лицо, реализующие в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой на бумажном носителе и (или) цифровым объектом, содержащим персональные данные;
15) **Согласие Субъекта** - подтвержденное Субъектом или его законным представителем разрешение на сбор и Обработку Персональных данных, предоставленное способом и в форме, позволяющих подтвердить его получение в соответствии с законодательством.
16) **Субъект Персональных данных** - физическое лицо, к которому относятся Персональные данные.
17) **Удаление Персональных данных** - исключение Персональных данных из цифрового объекта или базы без возможности восстановления
18) **Уничтожение Персональных данных** - действия, в результате которых невозможно восстановить Персональные данные.

19) **Цифровой объект, содержащий персональные данные** - цифровой объект, содержащий совокупность упорядоченных персональных данных.

3. Принципы Обработки Персональных данных

9. Группа осуществляет Сбор, Обработку и Защиту Персональных данных в соответствии с принципами, прямо установленными законодательством Республики Казахстан. С учетом международного характера деятельности Группы дополнительные принципы применяются в случаях, когда они предусмотрены применимым иностранным законодательством либо приняты Группой как более высокий стандарт защиты и не противоречат императивным требованиям законодательства Республики Казахстан.
10. Сбор, Обработка и защита Персональных данных в Группе осуществляются в соответствии со следующими принципами:
    1) **Соблюдение конституционных прав и свобод человека и гражданина.** Любое действие с Персональными данными должно учитывать право человека на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и достоинства, а также иные права и свободы. Обработка не должна создавать необоснованное, несоразмерное или дискриминационное вмешательство в частную жизнь Субъекта.
    2) **Законность.** Персональные данные собираются и обрабатываются только при наличии Согласия Субъекта или его законного представителя либо в случаях, когда Обработка без Согласия прямо допускается законодательством.
    3) **Конкретные, заранее определенные и законные цели.** До начала сбора и Обработки Персональных данных должна быть определена и задокументирована конкретная рабочая цель. Персональные данные используются только для ранее заявленных целей. Использование для новой цели допускается после проверки ее совместимости с первоначальной целью, наличия законного основания, необходимости уведомления Субъекта и, когда это требуется, получения нового Согласия.
    4) **Необходимость и достаточность.** Группа обрабатывает только те Персональные данные, которые объективно необходимы и достаточны для выполнения соответствующей задачи и включены в «Перечень Персональных данных, необходимый и достаточный для выполнения осуществляемых задач».
    5) **Достоверность, точность и актуальность.** Подразделения принимают разумные меры для проверки данных в зависимости от цели их использования, обеспечивают возможность исправления и дополнения и не используют заведомо недостоверные

или устаревшие сведения для принятия решений, способных затронуть права и интересы человека.

6) **Ограничение срока хранения.** Персональные данные хранятся не дольше, чем этого требуют цели Обработки, законодательство, договорные, претензионные и иные обязательства Группы. По окончании установленного срока данные подлежат Уничтожению, Удалению, Обезличиванию или иному предусмотренному законодательством преобразованию.
7) **Ограничение доступа и использование только в служебных целях.** Доступ к Персональным данным предоставляется по принципу служебной необходимости и в объеме, необходимом для конкретной роли. Запрещается обращаться к сведениям о пассажирах, работниках или иных лицах из личного интереса, по просьбе знакомых либо для целей, не связанных с должностными обязанностями.
8) **Конфиденциальность Персональных данных ограниченного доступа.** Работники, получившие доступ к Персональным данным ограниченного доступа, не вправе раскрывать, распространять, публиковать, пересылать или иным образом делать их доступными лицам, не имеющим соответствующих полномочий. Обязанность сохранять конфиденциальность продолжает действовать после прекращения трудовых, договорных или иных отношений с Группой.
9) **Прозрачность и информированность Субъекта.** В случаях и объеме, предусмотренных применимым законодательством, Субъекту предоставляется понятная информация о целях и способах Обработки, составе данных, возможных получателях, сроках или критериях хранения, правах и каналах обращения. Соответствующие уведомления о сборе и Обработке Персональных данных, а также формы Согласия не должны скрывать существенные условия, вводить Субъекта в заблуждение или понуждать его к предоставлению необязательных данных.
10) **Документирование и подтверждаемость соблюдения.** Структурные подразделения, в бизнес-процессах которых осуществляется Сбор и Обработка Персональных данных должны быть способны подтвердить, какие данные они обрабатывают, для какой задачи и цели, на каком основании, в какой системе, кому предоставляют, как защищают и когда удаляют.
11) **Защита на протяжении всего жизненного цикла.** Меры защиты применяются с момента сбора до окончательного Удаления, Уничтожения или Обезличивания данных и распространяются на получение, ввод, хранение, просмотр, изменение, выгрузку, передачу, архивирование и Удаление. При выборе меры учитываются категория и объем данных, способ Обработки, число лиц с доступом, использование внешних поставщиков, вопросы трансграничной передачи, и иные риски.

4. Роли и обязанности

4.1 Общие положения

11. Обеспечение соблюдения требований настоящей Политики и законодательства, а также управление рисками в области Персональных данных является частью общей системы корпоративного управления, управления рисками, комплаенс-контроля и информационной безопасности Группы.
12. В зависимости от характера конкретного процесса и требований применимого законодательства Группа может выступать в качестве Собственника и (или) Оператора Базы, содержащей Персональные данные, а в соответствии с применимым иностранным законодательством — в качестве контролера, совместного контролера, обработчика или стороны, выполняющей сопоставимые функции.
13. Каждый бизнес-процесс Сбора и Обработки Персональных данных должен иметь определенного Владельца бизнес-процесса.

4.2 Служба комплаенс/ Лицо, ответственное за организацию Обработки Персональных данных

14. В каждой компании Группы производственным приказом назначается Лицо, ответственное за организацию Обработки Персональных данных, в соответствии с требованиями законодательства Республики Казахстан.
15. В АО «Эйр Астана» такое лицо назначается в Службе комплаенс.
16. Служба комплаенс/Лицо, ответственное за организацию Обработки Персональных данных, осуществляет координационные и контрольные функции соблюдения требований настоящей Политики и законодательства и не заменяет Владельцев бизнес-процессов, Департамент информационных технологий (включая подразделение информационной безопасности) и иных участников процессов Обработки в части обязанностей и ответственности, возложенных на них настоящей Политикой и законодательством.

4.3 Владелец бизнес-процессов

17. Владелец бизнес-процесса отвечает за то, чтобы Сбор и Обработка Персональных данных в рамках соответствующего бизнес-процесса:
    - осуществлялись для конкретной, заранее определенной и законной цели;
    - имели надлежащее правовое основание;

- ограничивались Персональными данными, необходимыми и достаточными для выполнения соответствующей задачи;
- не продолжались дольше, чем это необходимо для достижения цели или выполнения требований законодательства;
- были обеспечены соответствующими организационными и техническими мерами защиты;
- соответствовали иным требованиям в области персональных данных, предусмотренным законодательством и настоящей Политикой, которые при необходимости детализируются Владельцем бизнес-процесса в процедурах, инструкциях либо иных внутренних нормативных документах, регулирующих соответствующий бизнес-процесс.

4.4 Департамент информационных технологий

18. Департамент информационных технологий, включая подразделение информационной безопасности осуществляет реализацию требований информационной безопасности в отношении Сбора и Обработки Персональных данных, включая:
    - Защиту Персональных данных;
    - механизмы идентификации, аутентификации, многофакторной аутентификации и управления доступом;
    - журналирование событий и действий пользователей;
    - шифрование, криптографическую защиту и защищенность каналов передачи;
    - управление уязвимостями и контроль установки обновлений средств защиты и программного обеспечения;
    - участие в расследовании Нарушений безопасности Персональных данных;
    - реализацию прочих соответствующих требований законодательства и настоящей Политики, при необходимости детализированных в процедурах, инструкциях либо иных внутренних нормативных документах Департамента информационных технологий.

4.5 Юридический департамент

19. Юридический департамент оказывает правовую поддержку по вопросам:
    - толкования законодательства Республики Казахстан и применимого иностранного законодательства в области Персональных данных;
    - подготовки типовых договоров и соглашений об Обработке Персональных данных;

- предоставления персональных данных по запросу правоохранительных и судебных органов;
- рассмотрения досудебных претензий, судебных споров;
- подготовки позиции Группы при взаимодействии с государственными органами, правовое сопровождение проверок уполномоченного органа;
- прочим соответствующим вопросам в рамках требований законодательства и настоящей Политики, при необходимости детализированным в процедурах, инструкциях либо иных внутренних нормативных документах Юридического департамента.

4.6 Работники Группы

20. Каждый работник Группы обязан соблюдать требования законодательства, настоящей Политики, а также процедур, инструкций и иных внутренних нормативных документов, регулирующих вопросы персональных данных в части, относящейся к выполняемой им деятельности.

5. Перечень Персональных данных, необходимый и достаточный для выполнения осуществляемых задач

21. В целях определения допустимого состава Персональных данных, собираемых и обрабатываемых в рамках деятельности Группы, Владельцы бизнес-процессов, в которых осуществляется сбор и Обработка Персональных данных, формируют и утверждают Перечень Персональных данных, необходимый и достаточный для выполнения осуществляемых задач (далее — Перечень).
22. Владельцы бизнес-процессов отвечают за полноту, точность и актуальность сведений в Перечне.
23. Шаблон Перечня приведен в **Приложении 1 к настоящей Политике.**

6. Основания для Сбора и Обработки Персональных данных

24. Сбор и Обработка Персональных данных осуществляются с Согласия Субъекта или его законного представителя, кроме случаев, когда Обработка без Согласия прямо допускается законодательством Республики Казахстан. В процессах, подпадающих под иностранное законодательство, дополнительно определяется соответствующее правовое основание.

25. Согласие и связанные доказательства его получения должны храниться в течение срока обработки и периода, необходимого для подтверждения соблюдения требований.

7. Сбор и Обработка копий документов, удостоверяющих личность, на бумажном носителе

26. Сбор и Обработка копий документов, удостоверяющих личность, на бумажном носителе не допускаются. При подтверждении личности предпочтение отдается проверке оригинала документа или цифрового документа, предъявленного посредством сервисов электронного правительства Республики Казахстан.

8. Управление рисками третьих сторон

27. Если взаимоотношения с третьей стороной предполагают сбор, получение, передачу, предоставление доступа или иную Обработку Персональных данных, Владелец бизнес-процесса обеспечивает включение в договор положений, регулирующих Обработку Персональных данных, в соответствии с требованиями законодательства и настоящей Политики.
28. В части положений, относящихся к Персональным данным, договор согласовывается со Службой комплаенс и, при необходимости, с подразделением информационной безопасности в части применяемых мер информационной безопасности.
29. Если передача Персональных данных осуществляется без заключения договора, в том числе государственным органам, авиационным властям, или иным уполномоченным получателям, Владелец бизнес-процесса обеспечивает наличие и документирование применимого правового основания такой передачи и соблюдение установленных законодательством требований к ее осуществлению.
30. Общая оговорка о конфиденциальности в договоре не заменяет специальные положения об Обработке Персональных данных.

9. Трансграничная передача персональных данных

31. Трансграничная передача Персональных данных осуществляется только при наличии предусмотренного законодательством правового основания и с соблюдением установленных законодательством условий и ограничений.

32. До осуществления трансграничной передачи Владелец бизнес-процесса обеспечивает определение:
    - цели и правового основания передачи;
    - страны, в которую передаются Персональные данные;
    - получателя Персональных данных;
    - категорий субъектов и состава передаваемых Персональных данных;
    - применимых требований и ограничений в отношении такой передачи.
33. В случаях, предусмотренных законодательством, до осуществления трансграничной передачи должны быть получены необходимые согласия субъектов Персональных данных и/или выполнены иные установленные законодательством условия.
34. Если трансграничная передача осуществляется в рамках договорных отношений, соответствующий договор должен предусматривать применимые требования к Обработке и защите Персональных данных.
35. Если трансграничная передача осуществляется без заключения договора, в том числе иностранным государственным органам, авиационным властям или иным уполномоченным получателям, такая передача допускается при наличии соответствующего правового основания и с соблюдением применимых требований законодательства.

10. Хранение, локализация и завершение жизненного цикла

36. Хранение Персональных данных в электронных информационных ресурсах осуществляется в Базе, находящейся на территории Республики Казахстан.
37. Персональные данные хранятся не дольше, чем это необходимо для достижения целей их Сбора и Обработки, если более длительный срок хранения не установлен законодательством Республики Казахстан, применимым иностранным законодательством, либо не обусловлен иной обоснованной необходимостью.
38. Владелец бизнес-процесса несет ответственность за определение, документирование и соблюдение срока хранения Персональных данных в рамках соответствующего бизнес-процесса.
39. По истечении установленного срока хранения Персональные данные подлежат Удалению, Уничтожению, Обезличиванию либо иному порядку действий, исключающему дальнейшую идентификацию Субъекта, если их дальнейшее хранение не требуется на законном основании.

11. Передача данных для статистических, социологических, научных и маркетинговых исследований

40. При передаче Персональных данных для проведения статистических, социологических, научных или маркетинговых исследований данные должны быть предварительно Обезличены, если передача сведений, позволяющих идентифицировать Субъектов, прямо не предусмотрена законодательством и не имеет отдельного надлежащего правового основания.

12. Права Субъектов и порядок рассмотрения обращений

41. Группа обеспечивает реализацию прав Субъектов Персональных данных в соответствии с законодательством Республики Казахстан, а в применимых случаях — с требованиями иностранного законодательства.
42. Реализация прав Субъекта Персональных данных либо отказ в их реализации по предусмотренным законодательством законным основаниям осуществляется в сроки, установленные законодательством. Соответствующий детализированный порядок, при необходимости отражается в процедурах, инструкциях либо иных внутренних нормативных документах профильных структурных подразделений.
43. Субъект вправе реализовать свои права лично либо через законного представителя. При обращении представителя Группа вправе запросить документы, подтверждающие его полномочия.

13. Нарушения безопасности и реагирование на инциденты

44. Работник обязан незамедлительно сообщить о фактическом или предполагаемом инциденте Нарушения безопасности Персональных данных в Службу комплаенс (data.privacy@airastana.com) и подразделение информационной безопасности (it.security@airastana.com).
45. При возникновении инцидента, связанного или потенциально связанного с Нарушением безопасности Персональных данных, Департамент информационных технологий осуществляет расследование, локализацию и устранение инцидента в соответствии с применимыми внутренними нормативными документами Департамента информационных технологий.

46. В контексте фактического или предполагаемого инцидента Нарушения безопасности Персональных данных Служба комплаенс в рамках своей компетенции обеспечивает соблюдение требований применимого законодательства в области Персональных данных, включая рассмотрение вопроса о необходимости уведомления уполномоченного органа и, при наличии соответствующей обязанности, организацию направления такого уведомления в установленный законодательством срок.
47. Служба комплаенс и Департамент информационных технологий взаимодействуют и обмениваются необходимой информацией в случаях, когда инцидент связан или потенциально может быть связан с Нарушением безопасности Персональных данных.
48. Детальный порядок регистрации, эскалации, расследования, взаимодействия и документирования инцидентов определяется соответствующими внутренними нормативными документами обозначенных структурных подразделений.

14. Ответственность

49. Нарушение законодательства в области персональных данных и/или настоящей Политики может повлечь дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством, а также причинить материальный и репутационный ущерб Группе.

15. Управление изменениями

50. Политика вступает в силу с даты ее утверждения Советом директоров АО «Эйр Астана».
51. Служба комплаенс обеспечивает пересмотр Политики не реже одного раза в три года и при существенных изменениях законодательства, бизнес-процессов, или уровня риска.
52. Если отдельное положение Политики становится неприменимым вследствие изменения законодательства, остальные положения сохраняют действие, а соответствующий вопрос регулируется законодательством до внесения изменений в Политику.

16. Ссылки

53. Политика разработана на основании и с учетом следующих нормативно-правовых актов в их действующей на момент утверждения Политики редакции:

- Конституция Республики Казахстан;
- Закон Республики Казахстан от 21 мая 2013 года № 94-V «О Персональных данных и их защите»;
- Закон Республики Казахстан от 24 июня 2026 года № 326-VIII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам цифровизации, защиты Персональных данных, дорожного движения и регулирования передовых технологий на транспорте» — в части положений, применяемых с даты их введения в действие;
- Правила сбора, Обработки Персональных данных, утвержденные приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ;
- Правила определения собственником и (или) оператором перечня Персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач, утвержденные приказом от 21 июня 2023 года № 199/НҚ;
- Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных, утвержденные приказом от 12 июня 2023 года № 179/НҚ, с учетом последующих изменений;
- Правила осуществления уведомления субъектов персональных данных о нарушении безопасности персональных данных, утвержденные приказом от 9 августа 2024 года № 481/НҚ, с учетом последующих изменений;

54. С учетом осуществления деятельности на международном рынке Группа также соблюдает ратифицированные Республикой Казахстан международные договоры и применимое законодательство иностранных государств в области Персональных данных, когда такое законодательство распространяется на деятельность Группы. К таким требованиям могут относиться законодательство в области защиты Персональных данных Европейского союза, Великобритании, Китайской Народной Республики и законы иных государств, в которых Группа осуществляет деятельность.

17. Правило разрешения противоречий

55. В случае противоречия между настоящей Политикой и применимым законодательством применяются требования законодательства. В случаях, когда Политика устанавливает более строгие требования к приватности или защите Персональных данных, применяются более строгие требования.

56. Требования иностранного законодательства не отменяют обязательные требования законодательства Республики Казахстан. При ситуациях потенциальных противоречий необходимо обратиться в Службу комплаенс (data.privacy@airastana.com) и Юридический департамент (legal@airastana.com)

История изменений		
Номер ревизии	**Изменения (только номер главы и наименование)**	**Дата вступления в силу**
v1	Новый документ	08.09.2022
v2	Добавлена RACI матрица в Разделе II; Добавлен Раздел X Контактная Информация; Добавлены Приложения 1,2; Обновлены Разделы V, VIII.	18.05.2023
v3	Политика пересмотрена и актуализирована с учетом изменений законодательства. Ее действие распространено на Группу Эйр Астана. Введены новые разделы о Перечне Персональных данных, основаниях Обработки, запрете сбора бумажных копий документов, локализации, сроках хранения и завершении жизненного цикла данных. RACI-матрица заменена разделом «Роли и обязанности». Удалены устаревшие положения. Обновлена терминология.	15.10.2026

Приложение 1.

Перечень Персональных данных, необходимый и достаточный для выполнения осуществляемых задач

№ п/п	Наименование задачи, в том числе функций, полномочий, обязанностей	Цели сбора и обработки в рамках осуществляемой задачи	Наименование Персональных данных для определенной цели	Указание на документы или нормативные правовые акты, имеющие прямые указания на осуществляемые собственником и (или) оператором задачи