Приложение
к Приказу АО «Казахтелеком»
от «18» октября 2021 года
№ 284

Политика по защите персональных данных в АО "Казахтелеком"

Алматы, 2021

Оглавление

1. Термины, сокращения и определения

Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.
АО «ГТС» - Акционерное общество «Государственная техническая служба».
Защита персональных данных (ЗПД) – комплекс мероприятий организационного, технического характера, направленных на защиту персональных данных.
ИБ – информационная безопасность.
Информация — сведения (сообщения, данные) независимо от формы их представления.
Использование персональных данных — действия (операции) с персональными данными, совершаемые работником Общества в целях принятия решений или совершения иных действий, необходимые в бизнес-процессах Общества.
КИБ – Комитет по информационной безопасности.
Конфиденциальность персональных данных — обязательство о недопущении лицами, получившими доступ к персональным данным, их распространения без согласия субъекта или иного законного основания.
МЦРиАП – Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.
НРД – нормативно-регламентирующая документация Общества (политики, стандарты, приказы, регламенты, руководства, инструкции и т.п.).
Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту.
Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с законами Республики Казахстан не распространяется требование соблюдения конфиденциальности.
Общество – Акционерное общество «Казахтелеком».
Персональные данные (ПД) — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), зафиксированные на электронном, бумажном и (или) ином материальном носителе.
Политика – утвержденная в Обществе настоящая Политика о защите персональных данных в АО «Казахтелеком».
Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных).
СП – структурное подразделение.
СП ИБ – структурное подразделение информационной безопасности;
Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной

системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2. Общие положения

1. Политика защиты персональных данных в АО «Казахтелеком» разработана с целью определения основных принципов обработки персональных данных клиентов, поставщиков, деловых партнеров, работников и других лиц, а также определяет основные действия по сбору, хранению и обработке персональных данных, меры по их защите в Обществе.

2. Политика является основополагающим документом в области защиты персональных данных, устанавливает цели, задачи и принципы в области защиты ПД, которыми руководствуется Общество в своей деятельности. Служит руководством при разработке соответствующих документов защиты персональных данных.

3. Нормативно-правовую основу настоящей Политики составляют Закон РК «О персональных данных и их защите» (далее - Закон), а также Правила сбора, обработки персональных данных, утвержденные приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 21.10.2020 №395/НҚ и НРД Общества.

4. Все работники, принимаемые на работу в Общество, обязаны ознакомиться с настоящей Политикой под роспись.

5. Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

3. Основные цели и задачи

6. Основными целями, на достижение которых направлены все положения настоящей Политики, являются:

1) непрерывность доступности ПД для поддержки бизнес-процессов Общества;

2) целостность ПД в целях поддержки высокого качества выполнения бизнес-процессов Общества;

3) конфиденциальность ПД;

4) соответствие предпринимаемых мер по ЗПД, применяемых в Обществе, требованиям законодательства РК, а также требованиям регулирующих и надзорных органов.

7. Основными задачами по реализации Политики являются планирование, реализация и контроль за выполнением комплекса организационных и технических мер по обеспечению ЗПД на основе оценки рисков Общества в сфере информационной безопасности, направленных на обеспечение:

1) защиты ПД от реальных и потенциальных угроз;

2) предупреждения, выявления и деактивации различных угроз;

3) установления причин и условий возникновения угроз;

4) быстрого реагирования на воздействия современных угроз и их точная локализация;

5) минимизация ущерба от событий, таящих угрозу безопасности ЗПД, посредством их предотвращения или сведения их последствий к минимуму;

6) применения современных международных методологий и практик по совершенствованию механизмов оперативного реагирования и расследования угроз;

7) эффективное управление рисками информационной безопасности;

8) обеспечение осведомленности работников о Политике, предпринимаемых мерах, требованиях по обеспечению ЗПД, обязанностях и правилах поведения, возлагаемых на работников Общества, а также обеспечение контроля за их надлежащим выполнением;

9) повышение уровня знаний и развитие корпоративной культуры в области ЗПД;

10) совершенствование ЗПД;

11) обеспечение соблюдения требований законодательства РК в ходе деятельности по обеспечению ЗПД в Обществе.

8. Для достижения указанных целей и решения перечисленных задач в Обществе строится ЗПД, соответствующая требованиям:

1) стандартов и законодательства РК в области ЗПД;

2) корпоративных нормативно-регламентирующих документов, договорных обязательств и иных нормативных документов в области ЗПД.

ЗПД, являясь частью общей системы управления Общества, документирована в настоящей Политике, а также в других документах ЗПД (частные политики, регламенты, руководства, стандарты, инструкции, положения, процедуры и т.п.), детализирующих, развивающих положения, изложенные в настоящей Политике на уровне их практической реализации и являющихся обязательными для всех работников Общества, а также представителей третьих сторон, имеющих доступ к ПД.

4. Сбор, обработка и защита персональных данных

9. Порядок получения (сбора) ПД:

1) все ПД субъекта следует получать у него лично с его письменного согласия или его законного представителя в порядке, определяемом уполномоченным органом, за исключением случаев, предусмотренных статьей 9 Закона;

2) согласие субъекта на использование его ПД хранится в бумажном виде, в личном деле абонента;

3) согласие субъекта на обработку ПД действует в течение всего срока действия договорных отношений субъекта с Обществом;

4) обработка ПД субъектов без его согласия осуществляется в следующих случаях:

- ПД являются общедоступными;

- по требованию полномочных государственных органов в случаях, предусмотренных законодательством РК;

- обработка ПД осуществляется для статистических целей при условии обязательного их обезличивания;

- в иных случаях, предусмотренных Законом.

10. Порядок обработки ПД:

1) субъект ПД предоставляет работнику Общества, ответственному за ведение операционной работы, сведения о себе;

2) на основании полученной информации работник Общества проверяет наличие данного субъекта, зарегистрированного в информационной системе Общества. Если субъект отсутствует в информационной системе Общества, то операционный работник заносит необходимую информацию о субъекте, после получения письменного согласия последнего. В случае наличия информации о субъекте в информационной системе Общества – сверяет данные с ранее предоставленными (при необходимости вносит соответствующие изменения);

3) обработка ПД субъекта может осуществляться исключительно в целях обеспечения выполнения бизнес-процессов с субъектом, с соблюдением законодательства РК и иных нормативных правовых актов;

4) объем и содержание обрабатываемых ПД должны быть достаточными для выполнения бизнес-процессов между субъектом ПД и Обществом и не превышать этот порог.

5) Перечень ПД необходимый и достаточный для выполнения осуществляемых задач, должен быть утвержден соответствующим распорядительным документом по Обществу, где данные обрабатываются, согласно Приложению к настоящей Политике.

11. Защита персональных данных:

1) под ЗПД субъекта понимается комплекс мер (организационно-распорядительных, технических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПД субъектов, а также от иных неправомерных действий со стороны лиц, не имеющих доступа к ПД;

2) Общество, в соответствии с законодательством РК, при ЗПД субъектов принимает все необходимые организационно-распорядительные и технические меры, в том числе:

- шифровальные (криптографические) средства;
- антивирусная защита;
- анализ уязвимостей;
- управление доступом;
- регистрация и учет;
- организация нормативно-методических мероприятий, регулирующих ЗПД.

5. Блокировка, обезличивание, уничтожение персональных данных

12. Порядок блокировки и разблокировки персональных данных:

1) блокировка ПД субъектов осуществляется с письменного заявления субъекта персональных данных;

2) блокировка ПД подразумевает:

- запрет редактирования ПД;
- запрет распространения ПД любыми средствами (e-mail, сотовая связь, информационные носители и т.д.);

3) блокировка ПД субъекта может быть временно снята, если это требуется для соблюдения законодательства РК;

4) разблокировка ПД субъекта осуществляется с его письменного согласия или заявления;

5) повторное согласие субъекта ПД на обработку его данных влечет разблокирование его ПД.

13. Порядок обезличивания и уничтожения ПД осуществляется на основании решения Комиссии по обезличиванию и уничтожению ПД (далее - Комиссия). Комиссия формируется на основании распорядительного документа по филиалу Общества, где обрабатывались ПД и должна состоять из Председателя Комиссии – работника, ответственного за организацию обработки ПД и работников филиала, имеющих доступ к ПД, в количестве не менее 3-х человек. Комиссия составляет соответствующий акт, который в последствии хранится у работника, ответственного за организацию обработки ПД в филиале Общества в отдельной папке. Обезличивание ПД субъекта происходит для проведения статистических, социологических, научных, маркетинговых исследований:

1) при обезличивании ПД в информационных системах заменяются набором символов, по которому невозможно определить принадлежность ПД к конкретному субъекту;

2) ПД подлежат уничтожению при истечении срока хранения ПД, при прекращении при прекращении правоотношений между субъектом, собственником ПД и Обществом, при вступлении в силу решения суда и в иных случаях, установленных Законом и иными нормативными правовыми актами РК;

3) бумажные носители документов при обезличивании ПД уничтожаются, также с составлением соответствующего акта, который в последствии хранится у работника, ответственного за организацию обработки ПД в филиале Общества в отдельной папке;

4) операция по обезличиванию и уничтожению ПД субъекта необратима и восстановлению не подлежит.

6. Передача и хранение персональных данных

14. Передача персональных данных:

1) под передачей ПД субъекта понимается распространение информации по каналам связи и на материальных носителях;

2) при передаче ПД работники Общества должны соблюдать следующие требования:

- осуществлять передачу ПД субъектов в пределах Общества в соответствии с настоящей Политикой, НРД и должностными инструкциями;

- разрешается доступ к ПД только тем работникам, с соответствующим уровнем доступа и объемом, которым необходимы ПД для выполнения должностных обязанностей;

- передавать ПД субъекта законным представителям субъекта в порядке, установленном законодательством РК и НРД и ограничивать эту информацию только теми ПД субъекта, которые необходимы для выполнения указанными представителями их функции.

15. Хранение и использование персональных данных:

1) под хранением ПД понимается существование записей в информационных системах и на материальных носителях;

2) ПД обрабатываются и хранятся в информационных системах, а также на бумажных носителях в Обществе;

3) хранение ПД ограниченного доступа в информационных системах осуществляется в базе расположенной на территории Республики Казахстан с использованием средств криптографической защиты информации, имеющих параметры не ниже третьего уровня безопасности;

4) срок хранения ПД осуществляется не дольше, чем этого требуют цели их сбора и обработки, но не менее двух лет, по истечении которых информация уничтожается.

7. Доступ к персональным данным

16. Предоставление доступа работнику Общества к ПД осуществляется согласно утвержденной Политике управления доступом к информационным ресурсам АО "Казахтелеком". Для этого необходимо выполнение одного из следующих условий:

1) доступ необходим для выполнения пользователем должностных обязанностей в соответствии со своим должностными инструкциями и полномочиями;

2) доступ необходим для выполнения пользователем обязанностей другого пользователя по поручению (в виде служебной записки) руководителя структурного подразделения;

3) доступ необходим для выполнения пользователем обязанностей другого пользователя по указанию (в виде приказа или распоряжения) руководства Общества;

4) доступ необходим для выполнения пользователем работ по указанию (в виде приказа или распоряжения) руководства Общества;

5) доступ необходим для выполнения пользователем работ в ходе реализации соглашений/ договоров, заключенных Обществом (для представителей третьих сторон).

8. Основные принципы обеспечения ЗПД

17. В основу настоящей Политики заложены следующие базовые принципы:

1) соблюдения конституционных прав и свобод человека и гражданина;
2) законность обеспечения ЗПД;
3) конфиденциальности ПД ограниченного доступа;
4) вовлеченность руководства Общества в процесс обеспечения ЗПД;
5) ориентированность на бизнес;
6) процессный подход;
7) комплексное использование способов, методов и средств защиты;
8) следование лучшим практикам;
9) разумная достаточность;
10) информированность и персональная ответственность.

9. Роли и ответственность

18. Контроль за выполнением требований настоящей Политики, а также за её актуальность и внесение изменений возлагается на СП ИБ.

19. Ответственность за обеспечение должного исполнения требований настоящей Политики возлагается на все заинтересованные СП в рамках их полномочий и в соответствии с положениями, установленными настоящей Политикой и разработанными на ее основе документами.

20. Руководители СП несут ответственность за своевременное доведение требований настоящей Политики до работников их подразделений и/или представителей третьих сторон в части, их касающейся, и за выполнение работниками их подразделений и/или представителями третьих сторон требований настоящей Политики.

21. Все пользователи должны быть ознакомлены с требованиями настоящей Политики.

22. Все пользователи ответственны за свои действия при использовании ПД в работе, а также за исполнение требований, установленных настоящей Политикой и внутренними документами, разработанными на ее основе.

23. В случае выявления нарушений требований настоящей Политики, которые повлекли несанкционированный доступ посторонних лиц при сборе, хранении, обработке ПД, должно быть инициировано и проведено служебное расследование с привлечением заинтересованных СП, а также представителей АО «ГТС», КИБ МЦРиАП.

24. Несоблюдение мер, предусмотренных настоящей Политикой, влечет за собой ответственность в соответствии с действующим законодательством РК и внутренними документами Общества.

10. Заключительные положения

25. Положения настоящей Политики подлежат пересмотру по результатам проведения внешнего аудита, внутреннего анализа и оценки рисков ИБ для информационной системы Общества, в результате каких-либо изменений в деятельности Общества, изменений в законодательстве РК и по мере необходимости.

26. Вопросы, не предусмотренные в положениях настоящей Политики, разрешаются в соответствии с законодательством РК, внутренними документами Общества (при этом законодательство РК имеет превалирующую силу).

27. Несоблюдение порядка и правил использования информационных ресурсов и принятых в Обществе мер по ЗПД влечет за собой ответственность в соответствии с действующим законодательством РК.

28. Настоящая Политика вступает в силу с момента ее утверждения и действует до принятия новой Политики.

29. Ответственность за внесение изменений в настоящую Политику несет руководитель СП ИБ.

30. Контроль за ознакомлением с настоящей Политикой возлагается на руководителя СП ИБ.

Приложение

к Политике по защите
персональных данных в АО
«Казахтелеком»

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