

АО «Казахский университет технологии и бизнеса
имени К. Кулажанова»

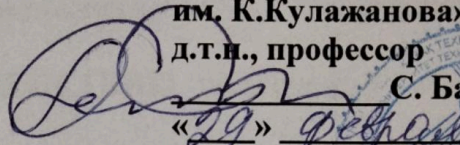
ПД 05-13.06-2022



Положение о защите персональных данных АО «КазУТБ
имени К. Кулажанова»

Редакция 4

Утверждаю
Президент-ректор
АО «Казахский университет
технологии и бизнеса
им. К.Кулажанова»
д.т.н., профессор


С. Байбеков
«29» февраля 2024 г.




ПОЛОЖЕНИЕ

О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ АО «КАЗАХСКИЙ УНИВЕРСИТЕТ ТЕХНОЛОГИИ И БИЗНЕСА ИМЕНИ К. КУЛАЖАНОВА»

Астана - 2024

©Является интеллектуальной собственностью АО «КазУТБ имени К. Кулажанова»
Перепечатка и/или дальнейшая передача третьим лицам запрещается.

АО «Казахский университет технологии и бизнеса имени К. Кулажанова»	ПД 05-13.06-2022	
Положение о защите персональных данных АО «КазУТБ имени К. Кулажанова»	Редакция 4	

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАНО И ВНЕСЕНО: Рабочей группой (РГ) совместно с отделом управления персоналом.

Руководитель РГ: Проректор по учебно-методической работе, PhD, Жамангарин Д.С.

Представитель РК: Проректор по учебно-методической работе, PhD, Жамангарин Д.С.

2. УТВЕРЖДЕНО И ВВЕДЕНО В ДЕЙСТВИЕ: решением Ученого совета № 7 протокола от «29» февраля 2024 г.

3. РАЗРАБОТЧИК: Отдел управления персоналом.

4. ПЕРИОДИЧНОСТЬ ПРОВЕРКИ: 3 года

5. ВВЕДЕНО ВЗАМЕН ПД: «Положение о защите персональных данных» ПД 05 – 13.09-2021, № 5 протокола от 28 декабря 2022 г.



СОДЕРЖАНИЕ

1. Общие положения	4
2. Нормативные ссылки	4
3. Сокращения и обозначения	4
4. Термины и определения	4
5. Понятие и состав персональных данных	6
6. Принципы обработки персональных данных	7
7. Доступ к персональным данным	8
8. Сбор персональных данных работников	8
9. Обработка персональных данных	9
10. Защита персональных данных	9
11. Обязанности Работодателя	9
12. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными	10
13. Изменения и дополнения	10
14. Согласование, хранение и рассылка	10
Приложение А Заявление о согласии на сбор, обработку персональных данных	11
Приложение Б Лист согласования	12
Приложение В Лист ознакомления	13
Приложение Г Лист регистрации изменений	14
Приложение Д Лист учета периодических проверок	15



1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее положение «О защите персональных данных» (далее - Положение) разработано с целью сбора, обработки, хранения и использования персональных данных работников и иных субъектов персональных данных АО «Казахский университет технологий и Бизнеса имени К. Кулажанова» (далее - Университет), гарантии защиты и конфиденциальности информации в соответствии с Конституцией РК, Трудовым кодексом РК, Законом РК «О персональных данных и их защите» и другими нормативными правовыми актами.

1.2 Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у работодателя, посредством планомерных действий по совершенствованию организации труда.

1.3 Положение является внутренним нормативным документом (далее - ВНД) Университета, предназначенным для руководства должностными лицами Университета и работниками Отдела.

1.4 Положение входит в комплект документации, принятого в Университете в соответствии с требованиями СМК.


2. НОРМАТИВНЫЕ ССЫЛКИ

2.1 В Положении приведены ссылки на следующие нормативно-правовые акты РК:

№	Наименование документов	Сведения об утверждении (№, дата)	Изменения и дополнения в нормативный документ (№, дата)
1.	Закон «О персональных данных и их защите»	№ 94-V от 21.05.2013 г.	по состоянию на 11.12.2023 г.
2.	Международный стандарт ISO 9000:2015 «Система менеджмента качества. Требования» (Quality management systems – Requirements, IDT)	№1390-ст от 28.09.2015 г.	
3.	Международный стандарт ISO 9000:2015 «Система менеджмента качества. Основные положения и словарь»	№1390-ст от 28.09.2015 г.	
4.	СТ РК ISO 9001:2016 «Система менеджмента качества. Требования»	№285-од от 14.11.2016 г.	

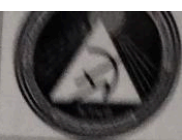
3. СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

ОБУиО	Отдел бухгалтерского учета и отчетности
ООКиА	Отдел обеспечения качества и аккредитации
ОУП	Отдел управления персоналом
РК	Республика Казахстан

«Казахский университет технологии и бизнеса имени К. Кулажанова»	ПД 05-13.06-2022	
Положение о защите персональных данных АО «КазУТБ имени К. Кулажанова»	Редакция 4	
ТК РК	Трудовой кодекс Республики Казахстан	
Университет	АО «Казахский университет технологии и бизнеса имени К. Кулажанова»	

4. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- 4.1 *Биометрические данные* - персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность.
- 4.2 *Персональные данные* - сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе:
- 4.2.1 *Государственный сервис контроля доступа к персональным данным* (далее – государственный сервис) – услуга, обеспечивающая информационное взаимодействие собственников и (или) операторов, третьих лиц с субъектом персональных данных и уполномоченным органом при доступе к персональным данным, содержащимся в объектах информатизации государственных органов и (или) государственных юридических лиц, включая получение от субъекта персональных данных согласия на сбор, обработку персональных данных или их передачу третьим лицам;
- 4.2.2 *Негосударственный сервис контроля доступа к персональным данным* (далее – негосударственный сервис) – услуга, обеспечивающая информационное взаимодействие собственников и (или) операторов, третьих лиц с субъектом персональных данных при доступе к персональным данным, содержащимся в негосударственных объектах информатизации, включая получение от субъекта персональных данных согласия на сбор, обработку персональных данных или их передачу третьим лицам;
- 4.2.3 *Блокирование персональных данных* - действия по временному прекращению сбора, накопления, изменения, дополнения, использования, распространения, обезличивания и уничтожения персональных данных;
- 4.2.4 *Накопление персональных данных* - действия по систематизации персональных данных путем их внесения в базу, содержащую персональные данные;
- 4.2.5 *Сбор персональных данных* - действия, направленные на получение персональных данных;
- 4.2.6 *Уничтожение персональных данных* - действия, в результате совершения которых невозможно восстановить персональные данные;
- 4.2.7 *Обезличивание персональных данных* - действия, в результате совершения которых определение принадлежности персональных данных субъекту персональных данных невозможно;
- 4.2.8 *База, содержащая персональные данные* (далее - база), - совокупность упорядоченных персональных данных;
- 4.2.9 *Собственник базы, содержащий персональные данные* (далее - собственник), - государственный орган, физическое и (или) юридическое лицо, реализующие в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные данные;
- 4.2.10 *Оператор базы, содержащий персональные данные* (далее - оператор), - государственный орган, физическое и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных;
- 4.2.11 *Защита персональных данных* - комплекс мер, в том числе правовых, организационных и технических, осуществляемых в целях, установленных настоящим Законом;
- 4.2.11.1 *Уполномоченный орган в сфере защиты персональных данных* (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство в сфере защиты персональных данных;



4.2.11.2 *Исключен* Законом РК от 30.12.2021 № 96-VII (вводится в действие по истечении шестидесяти календарных дней после дня его первого официального опубликования);

4.2.12 *Обработка персональных данных* – действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных;

4.2.13 *Использование персональных данных* – действия с персональными данными, направленные на реализацию целей деятельности собственника, оператора и третьего лица;

4.2.14 *Хранение персональных данных* – действия по обеспечению целостности, конфиденциальности и доступности персональных данных;

4.2.15 *Распространение персональных данных* – действия, в результате совершения которых происходит передача персональных данных, в том числе через средства массовой информации или предоставление доступа к персональным данным каким-либо иным способом;

4.2.16 *Субъект персональных данных* (далее – субъект) – физическое лицо, к которому относятся персональные данные;

4.2.17 *Третье лицо* – лицо, не являющееся субъектом, собственником и (или) оператором, но связанное с ними (ним) обстоятельствами или правоотношениями по сбору, обработке и защите персональных данных.

5. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

К персональным данным относятся:

- удостоверение личности или паспорт;
- документ об образовании, квалификации, наличии специальных знаний или профессиональной подготовки;
- документ, подтверждающий трудовую деятельность;
- документ воинского учета;
- документ о прохождении предварительного медицинского освидетельствования;
- справка подтверждающая регистрацию по месту жительства либо временного проживания;
- справка о наличии либо отсутствии судимости;
- трудовой договор и дополнительное соглашение к нему;
- письменное обращение;
- акты работодателя по личному составу;
- личные дела, личные карточки (форма Т2) и трудовые книжки сотрудников;
- другие документы, содержащие персональные данные и предназначенные для использования в служебных целях.

5.2 Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

5.3 Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом. Собственником информационных ресурсов (персональных данных) - является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с работодателем. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.



5.4 Держателем персональных данных является работодатель, которому сотрудник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

5.5 Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям - своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

5.6 Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

6. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение. Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

6.2 Все персональные данные сотрудника получаются у него самого. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Работодатель должен сообщить сотруднику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.

6.3 Не допускается получение и обработка персональных данных сотрудника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности. Пакет анкетно-биографических и характеризующих материалов (далее «Личное дело») сотрудника формируется в «Личное дело» после издания приказа о его приеме на работу.

6.4 «Личное дело» обязательно содержит личную карточку формы Т2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу: заявление сотрудника о приеме на работу; анкета; характеристика-рекомендация; результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей; копия приказа о приеме на работу; расписка сотрудника об ознакомлении с документами организации, устанавливающими порядок обработки персональных данных работников, а также об его правах и обязанностях в этой области; расписка сотрудника об ознакомлении его с локальными нормативными актами организации.

6.5 Все документы хранятся в файлах, файлы содержатся в папках в алфавитном порядке фамилий сотрудников. Анкета является документом «Личного дела», представляющим собой перечень вопросов о биографических данных сотрудника, его образовании, выполняемой работе с начала трудовой деятельности, семейном положении, месте прописки или проживания и т.п. Анкета заполняется сотрудником самостоятельно при оформлении приема на работу.

При заполнении анкеты и личной карточки Т2 используются следующие документы:

- паспорт;
- трудовая книжка;
- военный билет;



• документы об образовании.

«Личное дело» пополняется на протяжении всей трудовой деятельности сотрудника в данной организации. Изменения, вносимые в карточку Т2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

6.6 Работник ОУП, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами. При обработке персональных данных сотрудников работодатель в лице Президент-ректора вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников Университета на базе современных информационных технологий.

Сотрудник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен ТК РК;
- своевременно сообщать работодателю об изменении своих персональных данных.

Сотрудник имеет право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника. Доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия.

7. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1 Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри Университета исключительно для сбора, обработки и использования в работе.

1. Внешний доступ. К числу массовых потребителей персональных данных вне Университета можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- военкоматы;
- пенсионные фонды;

2. Внутренний доступ. Внутри Университета к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- все сотрудники отдела управления персоналом (далее - ОУП);
- все сотрудники отдела бухгалтерского учета и отчетности (далее - ОБУиО).

В ОУП хранятся личные карточки сотрудников, работающих в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные карточки располагаются в алфавитном порядке. После увольнения документы по личному составу передаются на хранение.

8. СБОР ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

8.1 Университет может получить все персональные данные о работнике от самого



работника;

8.2 Университет производит изменения персональных данных работника только на основании письменного заявления самого работника;

В случаях, когда Университет может получить необходимые персональные данные работника только у третьего лица, Университет должен уведомить об этом работника и получить от него письменное согласие;

8.3 Университет обязан сообщить работнику о целях, способах и источниках получения персональных данных, а так же о характере подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение.

9. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

9.1 Обработка персональных данных работника включает:

- накопление; хранение;
- изменение, дополнение;
- доступ;
- передача; распространение; трансграничная передача; обезличивание;
- блокирование; уничтожение.

9.2 Обработка персональных данных осуществляется с письменного согласия работников Университета на обработку их персональных данных.

10. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1 Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

10.2 Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

10.3 Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

11. ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ

11.1 Университет обязан:

- обеспечить и осуществлять сбор, обработку, передачу, хранение и защиту персональных данных работников в соответствии с законодательством РК о персональных данных и их защите, Конституцией РК, Трудовым кодексом РК и иными законами РК;
- при определении объема и содержания обрабатываемых персональных данных работника руководствуется Конституцией РК, Трудовым кодексом РК и иными законами РК;
- обрабатывать персональные данные, представленные уведомлением и получением согласия работника;
- обеспечить порядок хранения персональных данных работника с соблюдением требований, установленных законодательством РК о персональных данных и их защите;
- по требованию работника вносить изменения и дополнения в персональные данные работника в соответствии с законодательством РК о персональных данных и их защите;
- обеспечить ознакомление работника с актом работодателя, устанавливающим порядок сбора, обработки и защиты персональных данных в соответствии с законодательством РК;



- не сообщать персональные данные работника третьему лицу без письменного согласия работника, за исключением случаев, предусмотренных Трудовым кодексом и иными законами РК;
- разрешать доступ к персональным данным работника только специально уполномоченным лицам. При этом указанные должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций, и соблюдать режим конфиденциальности;
- осуществлять распространение персональных данных работника в пределах организации в соответствии с требованиями, установленными законодательством РК о персональных данных и их защите;
- предупреждать лиц, которым разрешен доступ к персональным данным работника, о том, что они обязаны использовать их исключительно в ранее заявленных целях и не передавать их третьим лицам, за исключением случаев, установленных законами РК.

12. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

12.1 Персональная ответственность—одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

12.2 Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

12.3 Каждый сотрудник, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

12.4 Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

13. ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ

13.1 В Положение могут вноситься изменения и дополнения, связанные с изменением законодательства, локальных нормативных актов, изменений структуры, которые утверждаются Президент-ректором Университета.

13.2 Изменения в Положение вносит разработчик с обязательной отметкой в «Листе регистраций изменений» (Приложение Г).

14. СОГЛАСОВАНИЕ, ХРАНЕНИЕ И РАССЫЛКА

14.1 Согласование Положения осуществляется с проректорами, руководителем ОУП, ОПО и оформляется в «Листе согласования».

14.2 Ответственность за хранение и рассылку учтенных рабочих экземпляров Положения должна осуществляться в ОУП.

14.3 За обеспечение и за сохранность копии рабочих экземпляров Положения несет руководитель ООКиА.

**Приложение А**

**Президент-ректору
АО «Казахский университет
технологии и бизнеса
им. К. Кулажанова»
С. Байбекову**

**ЗАЯВЛЕНИЕ
О СОГЛАСИИ НА СБОР, ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Я, _____, удостоверение _____
личности № _____, выданное _____ от «_____» 20_____ г. ИИН _____
в соответствии с подпунктом 24) пункта 1 статьи 22 и подпунктом 24) пункта 1 статьи 23
Трудового кодекса РК от 23 ноября 2015 года № 414-V, Закона РК от 21 мая 2013 года № 94-V
«О персональных данных и их защите», даю свое согласие на сбор, обработку АО «Казахский
университет технологии и бизнеса им. К. Кулажанова» (далее - Университет) моих
персональных данных, относящихся исключительно к перечисленным ниже категориям
персональных данных: фамилия, имя, отчество; пол; дата рождения; тип документа,
удостоверяющего личность; данные документа, удостоверяющего личность; гражданство;
информация о прохождении конкурса и тестирования; информация об отнесении к категории
лиц с ограниченными возможностями здоровья, инвалидов; информация о результатах
собеседования и, т.д.

Настоящее согласие предоставляется мной на осуществление действий в отношении
моих персональных данных, которые необходимы для достижения указанных выше целей,
включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение
(обновление, изменение), использование, передачу третьим лицам для осуществления
действий по обмену информацией, обезличивание, блокирование, защиту персональных
данных, а также осуществление любых иных действий, предусмотренных действующим
законодательством РК.

Я проинформирован, что Университет гарантирует обработку моих персональных
данных в соответствии с действующим законодательством РК, как неавтоматизированным,
так и автоматизированным способами. Данное согласие действует до достижения целей
обработки персональных данных или в течение срока хранения информации. Данное согласие
может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих
интересах.

Ф.И.О.

Подпись _____
(дата)

