Министерство образования и науки Республики Казахстан
АО «Университет КАЗГЮУ им. М.С. Нарикбаева»

АСАИНОВА ЛАУРА САБЫРБЕККЫЗЫ

Защита персональных данных в контексте использования технологий биометрической аутентификации

образовательная программа 7М04211 - «Юриспруденция»

Диссертация на соискание академической степени магистра юридических наук

Нур-Султан, 2021 г.

Министерство образования и науки Республики Казахстан
АО «Университет КАЗГЮУ им. М.С. Нарикбаева»

«Допущен к защите»
Руководитель/координатор программы
_____
«__» _____ 20__ г.
_____

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

На тему: «Защита персональных данных в контексте использования технологий биометрической аутентификации»

образовательная программа 7М04211 - «Юриспруденция»

Выполнил **Л.С. Асаинова**

Научный руководитель **докторант PhD**
Д.У. Мухамеджанова

Нур-Султан, 2021 г.

УТВЕРЖДАЮ
Руководитель/координатор
программы

_____
«__» _____ 20__ г.
_____

Календарный план подготовки магистерской диссертаций (проекта)

Наименование этапов проекта	Срок	Отметка о реализации этапов проекта			
		Фактический срок выполнения	Степень готовности выполненного этапа проекта	Подпись магистранта (магистрантов)	Подпись научного руководителя (научных руководителей)
Осуществление обзора литературы и практических материалов					
Разработка методологии					
Сбор и обработка данных					
Анализ и интерпретация полученных результатов					
Разработка рекомендаций по проекту					
Подготовка введения и заключения					
Оформление диссертаций (проекта): Подготовка I раздела проекта					

Подготовка II раздела проекта					
Подготовка III раздела проекта					
Получение отзыва научного руководителя (научных руководителей)					
Подготовка доклада, наглядных пособий и презентации					
Защита магистерской диссертаций (проекта)					

Научный руководитель магистерской диссертации (проекта)

_____

(Ф.И.О., должность и подпись)

План принял к исполнению:_____

(Ф.И.О. и подпись магистранта)

СОДЕРЖАНИЕ

Список сокращений

GDPR - The General Data Protection Regulation
CCPA - The California Consumer Privacy Act
РК - Республика Казахстан
РФ - Российская Федерация
ЕС - Европейский Союз
США – Соединенные Штаты Америки
ТК РК – Трудовой кодекс Республики Казахстан
КоАП РК – Кодекс об административных правонарушениях Республики Казахстан
УК РК – Уголовный кодекс Республики Казахстан
ЗРК – Закон Республики Казахстан
ФЗ РФ – Федеральный закон Российской Федерации
Пп. – подпункт
П. – пункт
Ст. - статья

Введение

Актуальность темы исследования. В декабре 2017 года Постановлением Правительства Республики Казахстан № 827 была утверждена Государственная программа «Цифровой Казахстан» 2018-2022 годы. Во исполнение данной программы государством осуществляется поддержка казахстанской стартап-культуры и перспективных высокотехнологичных IT-проектов в виде предоставления различного рода грантов, инвестиций и дотаций.

Для государственных органов данная программа выступает в качестве вектора дальнейшего развития, а для некоторых частных компаний и лиц в роли своеобразной подушки безопасности в процессе изобретения и внедрения новых технологий, в том числе технологий биометрической аутентификации.

В Казахстане более двадцати крупных компаний-работодателей активно внедряют на своих рабочих местах подобные технологии, фиксирующие учет рабочего времени работника посредством сбора его биометрических данных. Однако необходимо отметить, что на сегодняшний день отсутствуют четкие требования и правила обработки биометрических данных работника, которые включали бы в себя условия, при которых у работодателя возникает право требовать от работника предоставления его биометрических данных. Кроме того, законодателем также не урегулирован вопрос получения явного согласия работника на обработку его биометрических данных: достаточно ли подписания трудового договора работником или необходимо получение работодателем отдельного письменного согласия на обработку биометрических данных работника. Отсутствие конкретизации требований к процессу обработки работодателем биометрических данных работника и, как следствие, достаточных правовых механизмов защиты биометрических данных работника сопряжено как с риском несанкционированного сбора таких данных, так и с последствиями получения этих данных мошенниками.

Учитывая то, что технологии биометрической аутентификации имеют высокую скорость внедрения в сфере трудовых отношений, а законодательство не успевает регулировать каждый нюанс в полном объеме, появляется необходимость детального анализа проблемы обработки биометрических данных работника.

Целью исследования является выявление возможных правовых рисков, связанных с обработкой биометрических данных работников, с последующим внесением изменений и дополнений в соответствующие нормативные правовые акты в области защиты персональных данных работника.

Заданная цель диссертационной работы подразумевает решение следующих **задач**:

- проанализировать нормативные правовые акты Европейского Союза, Соединенных Штатов Америки, Российской Федерации и Республики Казахстан в области защиты биометрических персональных данных, уделяя особое внимание понятию «биометрических данных» и принципам сбора, обработки персональных данных;
- определить статусы Работника и Работодателя как субъектов института защиты биометрических данных;
- проанализировать потенциальные риски и последствия, сопряженные с нарушением правил обработки биометрических данных;
- изучить практику защиты биометрических данных работников в Европейском Союзе, Соединенных Штатах Америки, Российской Федерации и Республике Казахстан на предмет соблюдения принципов защиты персональных данных в области трудовых отношений;
- выработать рекомендации по совершенствованию действующего законодательства Республики Казахстан области защиты биометрических данных работников;

Предметом исследования являются биометрические данные работников.

Объектом исследования выступают общественные отношения в области защиты биометрических данных работников.

Нормативной (и практической) базой и иными дополнительными источниками исследования выступают: Закон Республики Казахстан «О персональных данных и их защите», Федеральный Закон Российской «О персональных данных», Калифорнийский закон по защите персональных данных - CCPA (California Consumer Privacy Act), Общий регламент защиты персональных данных GDPR (General Data Protection Regulation), Правила сбора, обработки персональных данных, Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных, Перечень персональных данных, необходимого и достаточного для выполнения осуществляемых задач, Правила проведения дактилоскопической и геномной регистрации, Правила сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг.

В диссертационном исследовании были использованы следующие **методы**: **сравнительному анализу** были подвергнуты законодательства Соединенных Штатов Америки (штата Калифорния), Европейского Союза, Российской Федерации и Республики Казахстан, регулирующие общественные отношения, связанные с обработкой и защитой биометрических данных работника; с помощью методов **идеализации** и

прогноза сформированы рекомендации по совершенствованию действующего законодательства Республики Казахстан области защиты биометрических данных работников.

Научная новизна диссертационного исследования заключается в ее практической значимости, основанной на предоставлении ряда рекомендаций, представленных в процессе анализа соответствующего материала. Данные рекомендации могут быть использованы законодателем для исключения и/или минимизации правовых рисков, сопряженных с нарушением правил обработки биометрических данных работника, и последующего совершенствования действующего законодательства Республики Казахстан области защиты биометрических данных работников.

На защиту выносятся следующие диссертационные положения:

1. Внесение в Закон Республики Казахстан N 94-V от 21 мая 2013 года «О персональных данных и их защите» изменений и дополнений, связанных с защитой персональных данных, в том числе введения видов «биометрических данных».

Внести дополнение в подпункт 1) пункт 1 Закона Республики Казахстан «О персональных данных и их защите» биометрические данные – персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность. К биометрическим данным относятся: изображение радужной оболочки глаза, изображение сетчатки глаза, отпечаток пальца, изображение лица, отпечаток ладони, отпечаток пальцев, рисунок вен, запись голоса, образцы нажатия клавиш, походка, данные о сне, данные о здоровье и др.

2. Внесение изменений и дополнений в Трудовой кодекс Республики Казахстан № 414-V ЗРК от 23 ноября 2015 года, направленных на защиту биометрических данных работника.

Внести дополнение в п. 1 ст. 32 Трудового Кодекса Республики Казахстан пп. 6) письменное согласие на сбор, обработку персональных данных работника в соответствии с Приложением № 1 к Правилам сбора, обработки персональных данных.

3. Внесение изменений и дополнений в следующие подзаконные акты:

1) в Правила сбора, обработки персональных данных, утвержденных Приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ;

2) Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных, утвержденных

Постановлением Правительства Республики Казахстан от 3 сентября 2013 года № 909;

3) Правила сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг, утвержденные Приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 406/НҚ;

4) Перечень персональных данных, необходимых и достаточных для выполнения осуществляемых задач, утвержденный Приказом Министра по инвестициям и развитию Республики Казахстан от 22 января 2018 года № 42.

4. Разработка типовой формы согласия работника на обработку его биометрических данных.

5. Разработка типовой формы запроса на получение доступа к базе персональных данных (подсистеме базы персональных данных).

6. Внесение изменений и дополнений в типовую форму Согласия на сбор и обработку персональных данных, утвержденную Правилами сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг

Теоретическая значимость исследования. Поднимаются актуальные проблемы обеспечения защиты персональных данных работника. Раскрываются решения проблемы нарушения порядка сбора, обработки биометрических данных работника. Работа может быть использована в дальнейших исследованиях.

Практическая значимость исследования. Предложенные в рамках исследования рекомендации, выступающие в качестве мер по улучшению эффективности процесса обработки и обеспечения гарантии защиты персональных данных, могут быть использованы в качестве основы для разработки поправок в законодательные акты Республики Казахстан по вопросам защиты персональных данных.

Структура диссертации состоит из: списка сокращений, введения, 2 разделов, заключения, библиографии и приложения.

РАЗДЕЛ I. БИОМЕТРИЯ: ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ И НОРМАТИВНОЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ

1.1. Этимология и история биометрии

Биометрия (в переводе с древнегреческого «bios» означает «жизнь», «metron» - «измерять»)[1]. Термин «Биометрия» использовался с первой половины XX-го века для обозначения области развития статистических и математических методов, применимых к задачам анализа данных в биологических науках. Сравнительно недавно термин «биометрия» стал также использоваться для обозначения области развития технологий, посвященных автоматической идентификации лиц, использующих уникальные биологические признаки человека, например, отпечатки пальцев, сетчатки или радужной оболочки, изображения лицах и т.д[2].

Международная организация по стандартизации (ISO) дает следующее определение биометрии: под «биометрией» понимается автоматическое распознавание людей на основе их биологических и поведенческих характеристик[3].

Помимо идентификации человека, как основной функции биометрических характеристик человека, они также могут выступать в качестве инструмента обеспечения безопасности какой-либо информации или предмета, имеющих определенную ценность для человека[4]. При этом стоит упомянуть, что биометрические системы идентификации и аутентификации личности отличаются от более традиционных форм обеспечения безопасности таких как, например, пароли, коды, параметры двухфакторной аутентификации.

Наиболее распространенными характеристиками распознавания человека являются его лицо, отпечаток пальца или радужная оболочка глаза, то есть физические особенности человека. Кроме того, благодаря продолжающимся на сегодняшний день исследованиям вводятся технологии, позволяющие использовать иные характеристики распознавания: рисунок вен, геометрия рук, ДНК или даже запах тела.

---

[1] Biometrics // https://searchsecurity.techtarget.com/definition/biometrics

[2] T. Ignatenko and F. M. J. Willems, Biometric Security from an Information-Theoretical Perspective, Foundations and Trends R in Communications and Information Theory, vol 7, nos 2–3, pp 135–316, 2010

[3] ISO/IEC 2382-37 // https://www.iso.org/standard/66693.html

[4] Асаинова Л.С. Биометрическая аутентификация как альтернативный способ идентификации человека. Научная статья. // http://scientificjournal.ru/a/116-yur/1464-biometricheskaya-autentifi.html

Поведенческая биометрия включает в себя модели почерка, голоса, нажатия клавиш и, например, походки.

За последние несколько тысячелетий биометрия прошла путь от грубых методов классификации до аутентификации личности с использованием самых разных методов.

Начиная с конца 1990-х годов, началась революция в области технологий распознавания личности. Биометрические технологии распознавания личности в некоторых случаях стали заменять более старые технологии идентификации и аутентификации личности[5].

Сканирование отпечатков пальцев и процесс распознавания лиц, которые лежат в основе современной революции в области биометрии предложили новаторам XIX века возможность идентификации преступников. Так, в 1880 году шотландский медицинский миссионер Генри Фолдс опубликовал в журнале «Nature» небольшое письмо с изложением его наблюдений относительно отпечатков пальцев, как приматов, так и человека, на древних гончарных изделиях. Господин Фолдс отметил, что эти «копии природы» можно сравнить визуально, что потенциально может привести к возможности «научной идентификации» преступников. Позже им была предложена система классификации отпечатков пальцев, которая положила начало столетним исследованиям других уникальных биологических факторов, которые можно было бы использовать в качестве инструментов идентификации[6].

Основные прорывы в биометрии произошли в 1900-х годах, включая использование рисунков радужной оболочки и геометрии руки для идентификации личности. В середине-конце 1900-х годов также зародилось движение распознавания лиц. В 1936 году Офтальмолог Фрэнк Берч впервые предложил идею использования рисунков радужной оболочки глаза в качестве метода идентификации. В 1960 году Шведский профессор Гуннар Фант представил модель, объясняющую физиологические компоненты производства акустической речи. Он проанализировал рентгеновские снимки людей, издающие определенные звуки, и основал на них свои выводы. Модель Фанта использовалась для лучшего понимания биологических компонентов речи, что является неотъемлемой концепцией распознавания говорящего[7].

В 1974 году стали доступны первые коммерческие системы распознавания геометрии руки. Такие системы преследовали три основные

---

[5] Mark Maguire. The birth of biometric security // https://www.researchgate.net/publication/249376012_The_birth_of_biometric_security

[6] Там же

[7] Там же

цели: учет времени и посещаемости, идентификация личности и контроль физического доступа.

В 2008 году Министерство обороны США и Федеральное бюро расследований начали разрабатывать базы данных, которые на сегодняшний день уже содержат в себе не только отпечатки пальцев, но также геометрию ладоней, лица и радужной оболочки глаза. С начала 2010-х годов биометрические технологии начали постепенно внедряться в частный сектор: Siri, Touch ID, Cortana[8].

1.2. Понятие и виды биометрической аутентификации

Биометрические технологии все чаще используются для распознавания людей и регулирования доступа к физическому пространству, информации, услугам и другим правам или преимуществам, включая возможность пересечения международных границ.

Системы, выполняющие биометрическое распознавание, существуют в группе других технологий аутентификации и идентификации. Технологии аутентификации, как правило, основаны на одной из трех вещей:

1) что-то, что человек знает, например, пароль;

2) что-то, что есть у человека, например, физический ключ или токен безопасности;

3) и что-то, кем человек является или то, что он делает.

Биометрические технологии относятся к последней группе. В отличие от систем, основанных на паролях или аппаратных токенах, биометрические системы могут функционировать без активного ввода, взаимодействия с пользователем или без знания того, что происходит распознавание. В основе биометрических технологий лежит процесс биометрической аутентификации.

Под биометрической аутентификацией понимается метод распознавания человека, имеющего доступ к защищенному активу, будь то физическое пространство, компьютерное программное обеспечение или оборудование, путем сравнения его уникальных биологических характеристик, таких как отпечатки пальцев, отпечаток ладони, сканирование сетчатки глаза или распознавание голосовых образов с соответствующими функциями в базе данных и предоставление человеку доступа только при совпадении[9].

---

[8] Stephen Mayhew. History of Biometrics // https://www.biometricupdate.com/201802/history-of-biometrics-2

[9] Subramanian N. (2011) Biometric Authentication. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA

Перед тем как непосредственно перейти к видам биометрической аутентификации необходимо решить вопрос с использованием необходимых в данной работе понятийных аппаратов, а именно разрешить вопрос значений терминов «идентификация», «аутентификация», «верификация» и «авторизация».

1.3. Понятие и виды биометрических данных: обзор законодательства ЕС (GDPR), США (CCPA, BIPA), РФ и РК

1.3.1. ЕС (GDPR)

В Европейском союзе почти с середины 2018 года действует «Общий регламент защиты персональных данных (GDPR) Европейского союза».

В данном Регламенте не просто регулируются механизмы защиты персональных данных человека, но и уделяется внимание биометрическим данным. Так, согласно подпункту 14) статьи 4 GDPR: «Биометрические данные» - это персональные данные, полученные в результате специальной технической обработки, которые касаются физических, физиологических или поведенческих черт физического лица, а также позволяют произвести или подтверждают однозначную идентификацию этого физического лица, например, изображение лица или дактилоскопические данные[10]

Также, согласно Преамбуле 51 GDPR, данные охватываются определением понятия «биометрические данные» только, когда они обрабатываются посредством специальных технических средств, позволяющих осуществить уникальную идентификацию или аутентификацию физического лица[11].

GDPR признает биометрические данные в качестве чувствительных персональных данных, однако отдельного от персональных данных в целом регулирования не предусматривает.

1.3.2. США (CCPA)

В США отсутствует федеральный закон по защите персональных данных. При этом в некоторых штатах существуют самостоятельные законы по защите персональных данных, например, в их числе штат Калифорния. Так, 01 января 2020 года в силу вступил Калифорнийский закон по защите персональных данных - CCPA (California Consumer Privacy Act), но некоторые положения CCPA устанавливают обязанность

[10] О GDPR на русском. Статья 4. Определения // https://ogdpr.eu/ru/gdpr-2016-679/chapter-1/statya-4-opredeleniya

[11] Статья 4 GDPR. Определения // https://gdpr-text.com/ru/read/article-4/

операторов по предоставлению субъектам персональных данных информацию о предшествующем 12-месячном периоде, следовательно, действия по соблюдению CCPA могут быть применены до даты вступления соответствующего закона в силу[12].

В США сложилась следующая практика принятия законов: после принятия штатом Калифорния какого-либо закона, многие другие штаты принимают подобные законы. Например, на сегодняшний день ведется разработка закона о защите персональных данных в штате Вашингтон. Однако создание пятидесяти отдельных законов в каждом штате было предотвращено началом ведения разработки соответствующего федерального закона. На данный момент на рассмотрении находятся два акта: Consumer Online Privacy Rights Act (COPRA), United States Consumer Data Privacy Act (CDPA). В качестве эталона и основополагающего образца выступает Калифорнийское законодательство.

В соответствии с разделом 1798 140(o)(1)(E)) биометрические данные признаются одним из видов персональных данных. В соответствии с разделом 1798 140 (b) под биометрическими данными понимаются физиологические, биологические или поведенческие характеристики человека, включая ДНК, которые могут использоваться, по отдельности или в сочетании друг с другом или с другими идентификационными данными, для установления личности. Биометрические данные включают в себя открытый перечень данных, которые закон подразделяет на два типа: 1) данные, из которых может быть извлечен шаблон идентификатора: изображение радужной оболочки глаза, изображение сетчатки глаза, отпечаток пальца, изображение лица, отпечаток ладони, отпечаток пальцев, рисунок вен, запись голоса; 2) которые могут быть биометрическими данными, если они содержат идентифицирующую информацию: Образцы нажатия клавиш, походка, данные о сне, данные о здоровье[13].

Первый тип биометрических данных, как правило, собираются для использования в технологиях аутентификации, например, для разблокировки устройства или получения доступа к информации или в помещение. Такие типы данных могут собираться производителями телефонов или разработчиками программного обеспечения безопасности. Работодатели также могут собирать эти типы биометрической информации для реализации ведения учета рабочего времени работников.

Второй тип данных может не собираться специально для целей идентификации или аутентификации, но может идентифицировать человека. Такие типы данных могут собираться устройствами для

---

[12] Comparing privacy laws: GDPR v. CCPA // https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

[13] California Consumer Privacy Act 2020 // https://oag.ca.gov/privacy/ccpa

отслеживания состояния здоровья или программным обеспечением, разработанным для интеграции с этими устройствами.

1.3.3. Российская Федерация

В соответствии с ч. 1 ст. 11 ФЗ РФ «О персональных данных» сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных ч. 2 настоящей статьи[14].

Постановление Правительства РФ № 772 от 30 июня 2018 года устанавливает следующий перечень биометрических персональных данных[15]:

1) данные изображения лица человека, полученные с помощью фото-, видеоустройств;

2) данные голоса человека, полученные с помощью звукозаписывающих устройств.

Кроме того, разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 августа 2013 года содержат в себе примерный перечень биометрических данных. Согласно вышеупомянутому подзаконному акту Российской Федерации к биометрическим персональным данным относятся[16]:

1) физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и др.);

2) иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта.

Крайне важно отметить, что данные разъяснения относятся к ненормативному правовому акту, так как его определенно можно отнести к письменному официальному документу, но который при этом не

---

[14] Статья 11 ФЗ РФ «О персональных данных» // https://base.garant.ru/12148567/9d78f2e21a0e8d6e5a75ac4e4a939832/

[15] Постановление Правительства РФ от 30 июня 2018 года № 772 // https://base.garant.ru/71979312/

[16] Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций // http://www.consultant.ru/document/cons_doc_LAW_151311/

устанавливает нормы права, а также не изменяет, дополняет, прекращает или приостанавливает действие этих норм.

Следовательно, перечень биометрических персональных данных должен изначально содержаться в нормативном правовом акте, а уже потом дублироваться в подзаконные акты в форме разъяснений.

1.3.4. Республика Казахстан

В Республике Казахстан действует Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите». В соответствии с пп. 1) ст. 1 вышеупомянутого закона под биометрическими данными понимаются персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность[17].

В нормативных правовых актах Республики Казахстан, как и в нормативных правовых актах Российской Федерации, отсутствует объемное понятие биометрических данных, которое включало бы конкретный перечень данных, под которыми законодатель понимает «биометрические данные».

Вывод № 1

Законодательством Республики Казахстан предусмотрен самостоятельный закон, регулирующий общественные отношения в области защиты персональных данных. Законом Республики Казахстан «О персональных данных и их защите» предусматривается признание биометрических данных персональными данными. Однако отдельного и узкоспециализированного регулирования непосредственно биометрических данных вышеупомянутым законом не предусматривается. Кроме того, законодателем также не представлена достаточная конкретизация, классификация видов биометрических данных как, например, в Калифорнийском законе по защите персональных данных.

2.2. Статусы Работника и Работодателя как субъектов института защиты биометрических данных

В соответствии с пп. 10) ст. 1 ЗРК «О персональных данных и их защите» оператор базы, содержащей персональные данные (далее –

---

[17] ЗРК «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094

оператор) – государственный орган, физическое и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных. В соответствии с пп. 16) ст. 1 Закона Республики Казахстан «О персональных данных и их защите» субъект персональных данных (далее – субъект) – физическое лицо, к которому относятся персональные данные[18].

Учитывая то, что Работодателю в соответствии с требованиями ст. 32 Трудового кодекса для заключения трудового договора необходимо запросить и ознакомиться с документами, содержащими персональные данные работника[19], Работодатель a priori осуществляет сбор и обработку персональных данных работника, следовательно, в соответствии с Законом «О персональных данных и их защите» выступает в качестве оператора.

Работодатель также может выступать в качестве собственника базы, содержащей персональные данные, так как может самостоятельно реализовывать в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные данные[20].

Работник в таком случае выступает субъектом персональных данных.

В соответствии с п. 1 ст. 22 ЗРК «О персональных данных и их защите» работодатель обязан принимать необходимые меры по защите персональных данных работника в соответствии с порядком, определяемым Правительством Республики Казахстан[21], обеспечивающие:

1) предотвращение несанкционированного доступа к персональным данным;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить;

3) минимизацию неблагоприятных последствий несанкционированного доступа к персональным данным;

4) предоставление доступа государственной технической службе к объектам информатизации, использующим, хранящим, обрабатывающим и распространяющим персональные данные ограниченного доступа, содержащиеся в электронных информационных ресурсах, для осуществления обследования обеспечения защищенности процессов

---

[18] ЗРК «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094

[19] Трудовой Кодекс Республики Казахстан № 414-V ЗРК от 23 ноября 2015 года // https://adilet.zan.kz/rus/docs/K1500000414#z32

[20] ЗРК «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094

[21] Правила сбора, обработки персональных данных // https://adilet.zan.kz/rus/docs/V2000021498

хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах в порядке, определяемом уполномоченным органом[22].

В соответствии с п. 2 ст. 25 ЗРК «О персональных данных и их защите» работодатель обязан[23]:

1) утверждать перечень персональных данных, необходимый и достаточный для выполнения осуществляемых ими задач, если иное не предусмотрено законами Республики Казахстан[24];

2) принимать и соблюдать необходимые меры, в том числе правовые, организационные и технические, для защиты персональных данных в соответствии с законодательством Республики Казахстан;

3) соблюдать законодательство Республики Казахстан о персональных данных и их защите;

4) принимать меры по уничтожению персональных данных в случае достижения цели их сбора и обработки, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;

5) представлять доказательство о получении согласия субъекта на сбор и обработку его персональных данных в случаях, предусмотренных законодательством Республики Казахстан;

6) сообщать информацию, относящуюся к субъекту, в течение трех рабочих дней со дня получения обращения субъекта или его законного представителя, если иные сроки не предусмотрены законами Республики Казахстан;

7) в случае отказа предоставить информацию субъекту или его законному представителю в срок, не превышающий трех рабочих дней со дня получения обращения, представлять мотивированный ответ, если иные сроки не предусмотрены законами Республики Казахстан;

8) в течение одного рабочего дня:

изменить и (или) дополнить персональные данные на основании соответствующих документов, подтверждающих их достоверность, или уничтожить персональные данные при невозможности их изменения и (или) дополнения;

блокировать персональные данные, относящиеся к субъекту, в случае наличия информации о нарушении условий их сбора, обработки;

---

[22] ЗРК «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094

[23] Там же

[24] Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных // https://adilet.zan.kz/rus/docs/P1300000909

уничтожить персональные данные в случае подтверждения факта их сбора, обработки с нарушением законодательства Республики Казахстан, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;

снять блокирование персональных данных в случае неподтверждения факта нарушения условий сбора, обработки персональных данных;

9) предоставлять безвозмездно субъекту или его законному представителю возможность ознакомления с персональными данными, относящимися к данному субъекту.

При этом обязанности работодателя по защите персональных данных возникают с момента сбора персональных данных и действуют до момента их уничтожения либо обезличивания[25].

В соответствии с п. 1 ст. 24 ЗРК «О персональных данных и их защите» работник имеет право:

1) знать о наличии у работодателя своих персональных данных, а также получать информацию, содержащую:

подтверждение факта, цели, источников, способов сбора и обработки персональных данных;

перечень персональных данных;

сроки обработки персональных данных, в том числе сроки их хранения;

2) требовать от работодателя изменения и дополнения своих персональных данных при наличии оснований, подтвержденных соответствующими документами;

3) требовать от работодателя блокирования своих персональных данных в случае наличия информации о нарушении условий сбора, обработки персональных данных;

4) требовать от работодателя уничтожения своих персональных данных, сбор и обработка которых произведены с нарушением законодательства Республики Казахстан, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;

5) отозвать согласие на сбор, обработку персональных данных, кроме случаев, предусмотренных п.2 ст. 8 ЗРК «О персональных данных и их защите»;

6) дать согласие (отказать) работодателю на распространение своих персональных данных в общедоступных источниках персональных данных;

7) на защиту своих прав и законных интересов, в том числе возмещение морального и материального вреда;

---

[25] Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094#z69

8) на осуществление иных прав, предусмотренных настоящим Законом и иными законами Республики Казахстан[26].

Вывод № 2

Нормы Закона Республики Казахстан «О персональных данных и их защите» распространяются как на работника, как на субъекта персональных данных, так и на работодателя, как на оператора базы, содержащей биометрические данные. Следовательно, работодатель обязан соблюдать не только требования Трудового кодекса, но и Закона Республики Казахстан «О персональных данных и их защите», а также соответствующих подзаконных актов.

3. Обработка биометрических данных: виды, цели и принципы сбора биометрических данных

Национальное законодательство устанавливает 5 принципов сбора, обработки и защиты персональных данных. В соответствии со ст. 5 ЗРК «О персональных данных и их защите» Сбор, обработка и защита персональных данных осуществляются в соответствии с принципами[27]:

1) соблюдения конституционных прав и свобод человека и гражданина;
2) законности;
3) конфиденциальности персональных данных ограниченного доступа;
4) равенства прав субъектов, собственников и операторов;
5) обеспечения безопасности личности, общества и государства.

Регламент (ЕС) 2016/679 Европейского Парламента и совета «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 / ЕС (Общие правила защиты данных)» устанавливает 6 принципов обработки персональных данных. В соответствии с п. 1 ст. 5 Регламента к персональным данным относятся[28]:

---

[26] ЗРК «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094

[27] Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094#z58

[28] Регламент (ЕС) 2016/679 Европейского Парламента и совета «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 / ЕС (Общие правила защиты данных)» // https://ogdpr.eu/ru/gdpr-2016-679/glava-2-printsipy/statya-5-printsipy-obrabotki-personalnyh-dannyh

a. обрабатываются законно, честно, в предусмотренной для субъекта данных форме («законность, честность и обзорность»);

b. собираются для конкретных, ясных и законных целей, и их дальнейшая обработка не осуществляется несовместимым с этими целями способом; дальнейшая обработка с целью архивирования в интересах общества, в целях научного или исторического исследования, или в целях статистики, согласно п. 1 ст. 89 не должна считаться несовместимой с первоначальными целями («целевые ограничения»)[29];

c. являются адекватными, соответствующими и включают только то, что необходимо для целей обработки («минимизация данных»);

d. являются точными и, при необходимости, обновлёнными; необходимо принимать все разумные меры для того, чтобы обеспечить немедленное удаление или исправление неточных данных, с учётом целей, для которых они обрабатываются («точность»)[30].

e. хранятся в форме, допускающей идентификацию субъектов данных, не дольше, чем это необходимо в целях, для которых обрабатываются персональные данные; персональные данные могут храниться дольше, если персональные данные будут обрабатываться только с целью архивирования в интересах общества, в целях научного или исторического исследования, или в целях статистики согласно пункту 1 Статьи 89 с условием, что будут приняты соответственные технические и организационные меры, предусмотренные настоящим регламентом для защиты прав и свобод субъекта данных («ограничение по хранению»)[31];

f. обрабатываются таким способом, чтобы была обеспечена безопасность персональных данных, в том числе защита от неразрешённой или незаконной обработки и от случайной потери, уничтожения или повреждения при проведении соответственных технических или организационных мер («целостность и конфиденциальность»).

---

[29] Статья 89 GDPR // https://gdpr-text.com/ru/read/article-89/

[30] Статья 5 GDPR // https://ogdpr.eu/ru/gdpr-2016-679/glava-2-printsipy/statya-5-printsipy-obrabotki-personalnyh-dannyh

[31] Статья 5 GDPR // https://gdpr-text.com/ru/read/article-5/

ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ДАННЫХ РАБОТНИКОВ

1. Потенциальные риски и последствия, сопряженные с нарушением правил обработки биометрических данных

Учитывая то, что свойства, которыми обладают биометрические данные, являются и их преимуществом, и их «ахиллесовой пятой», обеспечение безопасности биометрических данных сопряжено с множеством рисков неправомерного использования биометрических данных, которые можно подразделить на три категории: природная, правовая и технологическая.

В основе первой категории рисков лежит природа и особенность самих биометрических данных:

- биометрические данные обладают свойствами уникальности и неповторимости, позволяющие осуществлять процедуру идентификации и аутентификации физического лица;

- биометрическим данным свойственна физическая незащищенность: открытость пальцев рук позволяет другим лицам достаточно легко и без приложения особых усилий или технологий получить отпечаток пальцев человека. Такая незащищенность исключает само существование воли и волеизъявления субъекта персональных данных.

- свойства, которыми также обладают биометрические данные, это неизменность и природная врожденность, то есть низкая вероятность изменения «запрограммированных» биометрических данных. В отличие от других персональных данных, например, фамилии или имени, которые в дальнейшем могут быть относительно легко и быстро изменены, то изменения биометрических данных на данный момент возможны лишь при хирургическим вмешательстве.

В качестве последствия, сопряженного с первой категорией рисков, может выступить угроза того, что биометрические сведения могут стать инструментом дискриминации; например, информация, содержащаяся в ДНК, позволяет установить предрасположенность человека к определенным заболеваниям, что впоследствии может быть использовано в сфере трудоустройства или страхования[32].

---

[32] Кривогин М.С. Особенности правового регулирования биометрических персональных данных // https://cyberleninka.ru/article/n/osobennosti-pravovogo-regulirovaniya-biometricheskih-personalnyh-dannyh

Вторая категория рисков связана с отсутствием достаточного полного и всестороннего правового регулирования вопросов обеспечения защиты биометрических данных человека.

Проблемы безопасности биометрических систем можно отнести к третьей категории рисков.

Так, в 2005 году компания ChoicePoint, один из крупнейших накопителей данных и реселлеров в США, объявил, что мошенники смогли получить доступ к базе данных, содержащей информацию о 145000 потребителей. Компания была не в состоянии полностью идентифицировать частные лица и организации, купившие эту информацию, включая личные дела и номера социального страхования[33].

В 2007 году произошла крупнейшая утечка данных в финансовой сфере. Американский розничный гигант TJX объявил, что данные около 100 миллионов его клиентов был похищены. Хакеры проникли в беспроводную сеть компании и получили доступ к данным, передаваемым между переносными наладонными устройствами, считывающими цену, компьютерами магазина и кассовыми аппаратами. Компанию TJX критиковали за сбор избыточной информации, ее необоснованно долгое хранение, и за то, что она был не в состоянии улучшить безопасность своей беспроводной сети, перейдя от WEP-протокола шифрования (старый стандарт) к WPA, который намного более надежен. Компания TJX также подверглась нападкам за то, что слишком долго скрывал информацию о данном инциденте и не обеспечил соответствие стандартам безопасности данных индустрии платежных карт (PCI DSS). По оценкам некоторых экспертов, убытки TJX в результате данного инцидента составили более одного миллиарда долларов США[34].

На Филиппинах в феврале 2017 г. произошла утечка данных всех избирателей. В компьютере, который был украден из Комиссии по выборам, находилась биометрия (отпечатки пальцев) 55 миллионов граждан. Хотя данные были зашифрованы, нельзя исключать, что злоумышленники могли извлечь их[35].

---

[33] Астахов А. Искусство управления информационными рисками. // https://books.google.kz/books?id=1lydDQAAQBAJ&lpg=PP1&hl=ru&pg=PP1#v=onepage&q&f=false

[34] Риски утечки информации // http://xn----7sbab7afcqes2bn.xn--p1ai/content/riski-utechki-informacii

[35] Рассолов И.М., Чубукова С.Г., Микурова И.В. Биометрия в контекстсте персональных данных и генетической информации: правовые проблемы // https://cyberleninka.ru/article/n/biometriya-v-kontekste-personalnyh-dannyh-i-geneticheskoy-informatsii-pravovye-problemy

В январе 2021 года Народная прокуратура Шанхая обвинила двух жителей Китая в мошенничестве с системой распознавания лиц — Ву и Чжоу (фамилии Wu и Zhou) с 2018 года обманывали систему проверки личности налоговой службы и подделывали накладные[36].

Для обмана системы мошенники покупали фотографии в высоком качестве и поддельные личные данные на «чёрном онлайн-рынке», после чего обрабатывались в дипфейк-приложениях, которые могут «оживить» загруженную картинку и сделать из неё видео, создавая впечатление, что лица кивают, моргают, двигаются и открывают рот. Доступ к таким приложениям свободный и бесплатный[37].

Созданные видео мошенники загружали в специальные перепрошитые смартфоны, позволяющие во время распознавания лиц не включать фронтальную камеру: система получает заранее подготовленное видео, воспринимает его как изображение с камеры[38].

С помощью такой схемы мошенники зарегистрировали «компанию-пустышку», которая выдавала своим клиентам поддельные налоговые накладные. За два года мошенники заработали на этом 76,2 млн долларов США[39].

2. Судебная практика защиты биометрических данных

В данной работе предлагается рассмотреть судебное дело, непосредственно связанное с защитой биометрических данных казахстанского работника. Так, 7 марта 2017 года Темиртауским городским судом Карагандинской области было вынесено решение по иску г-на Паламарь Ю.А. (далее - Работник) к АО «АрселорМиттал Темиртау» (далее – Работодатель).

Работник требовал: 1) признать действия Работодателя по сбору, обработке биометрических данных Работника незаконными; 2) обязать Работодателя удалить собранные данные; 3) и взыскать с Работодателя моральный вред.

---

[36] Мошенники в Китае // https://vc.ru/legal/228953-moshenniki-v-kitae-s-pomoshchyu-dipfeykov-obmanuli-gossistemu-raspoznavaniya-lic-na-76-2-mln

[37] Мошенники в Китае // https://pulse.mail.ru/article/v-kitae-pojmali-moshennikov-kotorye-s-pomoschyu-dipfejkov-obmanuli-gossistemu-raspoznavaniya-lic-na-76-millionov-dollarov-65435613984874957-506895075424152725/

[38] Дипфейки // https://tgstat.com/uz/channel/@nauka_e

[39] Tax Scammers Hack Government-Run Facial Recognition System». South China Morning Post, 31 Mar. 2021, www.scmp.com/tech/tech-trends/article/3127645/chinese-government-run-facial-recognition-system-hacked-tax. Accessed 23 May 2021

Итак, Работник состоял в трудовых отношениях с Работодателем в период с 17 ноября 1995 года по 8 декабря 2016 года. Трудовой договор был расторгнут по соглашению сторон. Работник с соответствующим приказом был ознакомлен 8 декабря 2016 года.

В марте 2016 года Работодателем в соответствии с внутренним положением «О защите персональных данных» и коллективным договором была установлена СКД, которая посредством сбора персональных данных работников выполняет функции учета рабочего времени.

Несмотря на то, что согласно требованиям Коллективного договора Правление обязано письменно предупредить работника или профсоюз об изменении условий труда не позднее, чем за один месяц, Работников о введении СКД не уведомили.

Более того, с приказом Работодателя от 1 июня 2016 года об автоматизированном учете и оплате рабочего времени, а также с информационным письмом директора по производству от 18 марта 2016 года, о порядке применения Системы контроля доступа (далее - СКД), Работник был ознакомлен лишь при подписании соглашения о расторжении трудового договора, то есть 8 декабря 2016 года.

Необходимо также отметить, что приказ о введении системы учета рабочего времени был подписан неуполномоченным лицом, а изменение условий труда не было согласован с Профсоюзом.

Работодатель в свою очередь утверждает, что в соответствии с пп. 24) п. 2 ст. 23 ТК РК он имеет право осуществлять сбор, обработку и защиту персональных данных работника в соответствии с Законом о персональных данных. Работодатель в соответствии с ТК РК, являясь стороной трудового договора, является законным оператором персональных данных, в права и обязанности которого входит сбор, обработка, хранение персональных данных.

При этом учет рабочего времени Работника в соответствии с внутренним приказом Работодателя № 340 от 1 июня 2016 года ведется посредством технологий распознавания лиц. Соответствующая база изображений лиц работников сформирована за счет фотографий на пропусках.

По мнению профсоюза нарушений со стороны Работодателя не имеется, так как Работник дал свое согласие на сбор и обработку персональных данных при заключении трудового договора.

В своем решение суд указал следующее:

Учет рабочего времени является обязанностью работодателя, а форма и порядок ведения учета рабочего времени определяется внутренним актом работодателя. Следовательно, суд полагает, что действия Работодателя по установлению автоматизированной системы учета и оплаты рабочего

времени соответствуют требованиям закона и являются исключительным правом работодателя.

По мнению суда, отсутствие согласия Работника на обработку и хранение его персональных данных не является нарушением его прав, «поскольку в соответствии с пп. 24) п.2 ст. 23 ТК РК сбор, обработка и защита персональных данных работника в соответствии с законодательством Республики Казахстан о персональных данных и их защите, является обязанностью работодателя. Перечень документов, необходимых для заключения трудового договора перечислены ст. 32 ТК РК, где помимо документов удостоверяющих личность, также требуются ряд документов содержащих личные персональные данные».

Таким образом, суд приходит к выводу, что работодатель имел законные основания на сбор, обработку и хранение личных персональных данных Работника.

При этом исковые требования в части принудительного уничтожения Работодателем собранных им биометрических данных суд считает подлежащим удовлетворению, поскольку в судебном заседании установлено и представителем ответчика не опровергнуто, что такие данные у Работодателя имеются. В данном случае, суд руководствовался п. 2 ст. 12 Закона Республики Казахстан «О персональных данных и их защите». В соответствии с данной нормой срок хранения персональных данных определяется датой достижения целей их сбора и обработки, если иное не предусмотрено законодательством Республики Казахстан.

«Таким, образом, принимая во внимание прекращение трудовых отношений между Работником и Работодателем, суд приходит к выводу, что биометрические данные Работника с системы СКД подлежат уничтожению.

Вывод № 3

Данное дело может послужить наглядным примером того, что отсутствие в нормативных правовых актах в сфере трудовых отношений требования об обязательном наличии отдельного письменного согласия работника на сбор и обработку его персональных биометрических данных дает как работодателям, так и судам основание полагать, что заключение трудового договора является достаточным для открытия доступа к процессу сбора и обработки данных работника. Такое понимание противоречит требованиям ст. 8 ЗРК «О персональных данных и их защите». В соответствии со ст. 8 согласие субъекта на обработку его персональных данных является письменным.

Вышеупомянутый закон устанавливает перечень случаев, при которых сбор, обработка персональных данных производятся без согласия субъекта. К сожалению, данный перечень не является исчерпывающим, но, исходя из перечисленных в ст. 9 случаев, можно сделать вывод о том, что основания подпадают скорее под специализацию государственного сектора, нежели частных компаний. Следовательно, суд в действиях Работодателя мог усмотреть нарушение ст. 8 ЗРК.

Помимо этого, данное дело также подтверждает практическую необходимость наличия типовой формы письменного согласия на сбор, обработку персональных данных. Так, в данном деле Работник сфотографировался на пропуск, однако на тот момент целью сбора и обработки данного изображения лица не был учет рабочего времени Работника. Следовательно, несмотря на то, что цель использования биометрических данных Работника изменилась, соответствующего согласия Работника Работодатель не получал.

Суд посчитал, что Работник имеет право требовать уничтожения своих биометрических данных в связи с тем, что цель их сбора и обработки была достигнута, однако о том, какой именно была цель, остается лишь гадать и уповать на мнение суда: «трудовые отношения прекращены в связи с расторжением трудового договора – цель сбора, обработки персональных данных работника достигнута».

3. Ответственность за нарушение обработки биометрических данных работников

В соответствии со статьей 29 Закона Республики Казахстан «О персональных данных и их защите» нарушение законодательства Республики Казахстан о персональных данных и их защите влечет ответственность в соответствии с законами Республики Казахстан[40].

В соответствии с пп. 7) п. 1 ст. 24 Закона Республики Казахстан «О персональных данных и их защите» субъект имеет право на защиту своих прав и законных интересов, в том числе возмещение морального и материального вреда[41].

Статьей 79 Кодекса об Республики Казахстан об административных правонарушениях предусмотрена ответственность за незаконные сбор и (или) обработку персональных данных. Ответственность имеет денежный

---

[40] Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» // https://adilet.zan.kz/rus/docs/Z1300000094#z58

[41] Там же

характер. Максимальная административная ответственность – это штраф в размере 1 000 МРП[42].

Уголовный кодекс предусматривает ответственность за незаконное собирание сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконных сбора и (или) обработки иных персональных данных. Санкция за такое нарушение имеет альтернативный характер: штраф в размере до 5 000 МРП либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до 800 часов, либо ограничением свободы на срок до 3-х лет, либо лишением свободы на тот же срок[43].

4.1. Рекомендации для работодателя

В соответствии с п. 2 ст. 20 ЗРК «О персональных данных и их защите» сбор и обработка персональных данных осуществляются только в случаях обеспечения их защиты. Под обеспечением защиты предлагается понимать систему оценки рисков нарушения законодательства в области защиты персональных данных:

Во-первых, работодателю, как оператору базы, содержащей персональные данные, необходимо ввести отдельные позиции работников, осуществляющих сбор и обработку биометрических данных работников, путем их классификации на соответствующие категории. Категории работников должны соответствовать виду биометрических данных, к которым у них есть доступ, и осуществляемых с такими данными действий, например:

1) «работники категории 1-F»[44] - лица, имеющие исключительные полномочия на осуществление сбора биометрических данных работника (изображение лица);

1-1) «работники категории 1-I»[45] - лица, имеющие исключительные полномочия на осуществление сбора биометрических данных работника (радужка глаза);

1-2) «работники категории 1-R»[46] - лица, имеющие исключительные полномочия на осуществление сбора биометрических данных работника (сетчатка глаза);

---

[42] КоАП // https://adilet.zan.kz/rus/docs/K1400000235

[43] УК РК // https://adilet.zan.kz/rus/docs/K1400000226

[44] FI – Faceprint

[45] I – Imagery of the iris

[46] R - Retina

1-3) «работники категории 1-FP»[47] - лица, имеющие исключительные полномочия на осуществление сбора биометрических данных работника (отпечаток пальца);

2) «работники категории 2-F» - лица, имеющие исключительные полномочия на обезличивание биометрических данных работника (изображение лица);

2-1) «работники категории 2-I» - лица, имеющие исключительные полномочия на обезличивание биометрических данных работника (радужка глаза);

2-2) «работники категории 2-R» - лица, имеющие исключительные полномочия на обезличивание биометрических данных работника (сетчатка глаза);

2-3) «работники категории 2- FP» - лица, имеющие исключительные полномочия на обезличивание биометрических данных работника (отпечаток пальца);

3) «работники категории 3-FID»[48] - лица, имеющие исключительные полномочия на принятие решения о снятии обезличивания биометрических данных работника (изображение лица);

3-1) «работники категории 3-F» - лица, имеющие исключительные полномочия на снятие обезличивания биометрических данных работника (изображение лица);

3-2) «работники категории 3-ID» - лица, имеющие исключительные полномочия на принятие решения о снятии обезличивания биометрических данных работника (радужка глаза);

3-3) «работники категории 3-I» - лица, имеющие исключительные полномочия на снятие обезличивания биометрических данных работника (радужка глаза);

3-4) «работники категории 3-RD» - лица, имеющие исключительные полномочия на принятие решения о снятии обезличивания биометрических данных работника (сетчатка глаза);

3-5) «работники категории 3-R» - лица, имеющие исключительные полномочия на снятие обезличивания биометрических данных работника (сетчатка глаза);

3-6) «работники категории 3-FPD» - лица, имеющие исключительные полномочия на принятие решения о снятии обезличивания биометрических данных работника (отпечаток пальца);

---

[47] FP - Fingerprint

[48] D – Decision

3-7) «работники категории 3-FP» - лица, имеющие исключительные полномочия на снятие обезличивания биометрических данных работника (отпечаток пальца);

4) «работники категории 4-FD» - лица, имеющие исключительные полномочия на принятие решения об уничтожении биометрических данных работника (изображение лица);

4-1) «работники категории 4-F» - лица, имеющие исключительные полномочия на уничтожение биометрических данных работника (изображение лица);

4-2) «работники категории 4-ID» - лица, имеющие исключительные полномочия на принятие решения об уничтожении биометрических данных работника (радужка глаза);

4-3) «работники категории 4-I» - лица, имеющие исключительные полномочия на уничтожение биометрических данных работника (радужка глаза);

4-4) «работники категории 4-RD» - лица, имеющие исключительные полномочия на принятие решения об уничтожении биометрических данных работника (сетчатка глаза);

4-5) «работники категории 4-R» - лица, имеющие исключительные полномочия на уничтожение биометрических данных работника (сетчатка глаза);

4-6) «работники категории 4-FPD» - лица, имеющие исключительные полномочия на принятие решения об уничтожении биометрических данных работника (отпечаток пальца);

4-7) «работники категории 4-FP» - лица, имеющие исключительные полномочия на уничтожение биометрических данных работника (отпечаток пальца);

Перед представлением следующей категории работников работодателю, как собственнику базы, содержащей персональных данных, необходимо разделить базу, содержащую биометрические данные работников на четыре отдельные самостоятельные подсистемы, содержащие в себе: а) подсистема, содержащая биометрические данные работника (изображение лица); б) подсистема, содержащая биометрические данные работника (радужка глаза); в) подсистема, содержащая биометрические данные работника (сетчатка глаза); г) подсистема, содержащая биометрические данные работника (отпечаток пальца).

5) «работники категории – FI» - лица, обладающие исключительным правом доступа в подсистему базы данных с биометрическими данными работника (изображение лица);

5-1) «работники категории – I» - лица, обладающие исключительным правом доступа в подсистему базы данных с биометрическими данными работника (радужка глаза);

5-2) «работники категории – R» - лица, обладающие исключительным правом доступа в подсистему базы данных с биометрическими данными работника (сетчатка глаза);

5-3) «работники категории – FP» - лица, обладающие исключительным правом доступа в подсистему базы данных с биометрическими данными работника (отпечаток пальца).

* Лица, не имеющие соответствующих исключительных полномочий для осуществления действий, связанных с биометрическими данными работников, не имеют права осуществлять такие действия. Лица, которые не имеют исключительных полномочий доступа и работы с биометрическими данными работников, обязаны направлять официальный запрос работнику соответствующей категории.

** Один сотрудник имеет право доступа только к одному виду биометрических данных.

Перед получением допуска к работе с биометрическими данными работники обязаны:

1) пройти соответствующее обучение с целью получения теоретических знаний в области защиты биометрических данных, а также овладения определенными практическими навыками сбора, обработки и защиты биометрических данных;

2) после завершения обучения успешно пройти соответствующее тестирование, прохождение которого гарантирует освоение работником достаточного уровня знаний и навыков;

С целью реализации второго пункта работодателю необходимо разработать структуру тестирования, включающую в себя психологическое тестирование. Необходимо также установить пороговый уровень прохождения тестирования, например, 70 % из 100 %;

3) ежегодно два раза в год посещать краткосрочные, например, недельные, обучающие семинары, проходящие на территории Казахстана;

4) ежегодно один раз в год проходить аттестацию, по результатам которой комиссией будет принято соответствующее решение.

С целью реализации четвертого пункта необходимо разработать и утвердить Правила проведения аттестации работников, имеющих доступ к персональным данным работников.

Введение подобной классификации работников вводит не только элемент прозрачности «перемещения» персональных данных работников, но и элемент дисциплинированности как в деятельности работодателя,

принявшего решения использовать технологии биометрической аутентификации, так и деятельность работников, имеющих доступ к биометрическим данным. Открытость и, как следствие, более высокая вероятность снижения «локальной» утечки данных, то есть кражи самими работниками компании, оправдывает высокие требования, предложенные в настоящем исследовании.

4.2. Рекомендации по совершенствованию действующего законодательства Республики Казахстан области защиты биометрических данных работников

Настоящая редакция	Предлагаемая редакция
В соответствии со ст. 5 ЗРК «О персональных данных и их защите» Сбор, обработка и защита персональных данных осуществляются в соответствии с принципами: 1) соблюдения конституционных прав и свобод человека и гражданина; 2) законности; 3) конфиденциальности персональных данных ограниченного доступа; 4) равенства прав субъектов, собственников и операторов; 5) обеспечения безопасности личности, общества и государства[49]	В соответствии со ст. 5 ЗРК «О персональных данных и их защите» Сбор, обработка и защита персональных данных осуществляются в соответствии с принципами: 1) соблюдения конституционных прав и свобод человека и гражданина; 2) законности; 3) конфиденциальности персональных данных ограниченного доступа; 4) равенства прав субъектов, собственников и операторов; 5) обеспечения безопасности личности, общества и государства.[50] 6) целевое назначение: персональные данные собираются для конкретных, ясных и законных целей, и их дальнейшая обработка не осуществляется несовместимым с этими целями способом; 7) минимизация сбора данных, необходимых и достаточных для конкретной цели обработки таких

[49] ЗРК «О персональных данных и их защите» https://adilet.zan.kz/rus/docs/Z1300000094

[50] Там же

	данных; 8) ограничение доступа к базе персональных данных.
В соответствии с п. 1 ст. 8 ЗРК «О персональных данных и их защите» Субъект или его законный представитель дает (отзывает) согласие на сбор, обработку персональных данных письменно, в форме электронного документа или посредством сервиса обеспечения безопасности персональных данных либо иным способом с применением элементов защитных действий, не противоречащих законодательству Республики Казахстан[51].	В соответствии с п. 1 ст. 8 ЗРК «О персональных данных и их защите» Субъект или его законный представитель дает (отзывает) согласие на сбор, обработку персональных данных письменно, в форме электронного документа или посредством сервиса обеспечения безопасности персональных данных либо иным способом с применением элементов защитных действий, не противоречащих законодательству Республики Казахстан. [52] Согласие должно соответствовать Приложению № 1 Правил сбора, обработки персональных данных.
В соответствии с п. 2 ст. 25 ЗРК «О персональных данных и их защите» собственник и (или) оператор обязаны: 4-1) -	В соответствии с п. 2 ст. 25 ЗРК «О персональных данных и их защите» собственник и (или) оператор обязаны: 4-1) В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати календарных дней с даты поступления указанного отзыва.
В соответствии с п. 2 ст. 25 ЗРК «О персональных данных и их	В соответствии с п. 2 ст. 25 ЗРК «О персональных данных и их

[51] ЗРК «О персональных данных и их защите» https://adilet.zan.kz/rus/docs/Z1300000094

[52] Там же

защите» собственник и (или) оператор обязаны: 4-3) -	защите» собственник и (или) оператор обязаны: 4-1) представлять субъекту персональных данных в ответ на соответствующее обращение об уничтожении персональных данных доказательство об уничтожении его персональных данных.
В соответствии с п. 1 ст. 32 ТК РК для заключения трудового договора необходимы следующие документы: 6) -	В соответствии с п. 1 ст. 32 ТК РК для заключения трудового договора необходимы следующие документы: 6) письменное согласие на сбор, обработку персональных данных работника в соответствии с Приложением № 1 к Правилам сбора, обработки персональных данных.
В соответствии с п. 8 гл. 2 Правил сбора, обработки персональных данных для сбора персональных данных собственник и (или) оператор, а также третье лицо запрашивают у субъекта согласие на сбор, обработку отнесенных к нему персональных данных в порядке, определяемом настоящими Правилами.[53]	В соответствии с п. 8 гл. 2 Правил сбора, обработки персональных данных для сбора персональных данных собственник и (или) оператор, а также третье лицо запрашивают у субъекта согласие на сбор, обработку отнесенных к нему персональных данных в порядке, определяемом настоящими Правилами в соответствии с Приложением № 1 к настоящим Правилам [54]

[53] Правила сбора, обработки персональных данных // https://adilet.zan.kz/rus/docs/V2000021498

[54] Там же

Заключение

В результате проведенного анализа национального законодательства, эталонного законодательства Соединенных штатов Америки, Европейского Союза и Российской Федерации в области защиты персональных данных, а также соответствующей судебной практики, мы приходим к выводу, что биометрические данные являются чувствительными персональными данными, нуждающимися в отдельном правовом регулировании. Для минимизации и/или исключения указанных выше рисков и последствий, сопряженных с нарушением порядка и правил сбора, обработки биометрических данных работника, необходимо внести дополнения и изменения в следующие нормативные правовые акты Республики Казахстан: Трудовой Кодекс, Закона «О персональных данных и их защите». Кроме того, соответствующие изменения и дополнения также необходимо внести в такие подзаконные акты, как: Правила сбора, обработки персональных данных и Правила сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг.

Таким образом, в рамках проведенного исследования предлагается введение следующих изменений и дополнений:

1. Внесение в Закон Республики Казахстан N 94-V от 21 мая 2013 года «О персональных данных и их защите» изменений и дополнений, связанных с защитой персональных данных, в том числе введения видов «биометрических данных».

Внести дополнение в подпункт 1) пункт 1 Закона Республики Казахстан «О персональных данных и их защите» биометрические данные – персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность. К биометрическим данным относятся: изображение радужной оболочки глаза, изображение сетчатки глаза, отпечаток пальца, изображение лица, отпечаток ладони, отпечаток пальцев, рисунок вен, запись голоса, образцы нажатия клавиш, походка, данные о сне, данные о здоровье и др.

2. Внесение изменений и дополнений в Трудовой кодекс Республики Казахстан № 414-V ЗРК от 23 ноября 2015 года, направленных на защиту биометрических данных работника.

Внести дополнение в п. 1 ст. 32 Трудового Кодекса Республики Казахстан пп. 6) письменное согласие на сбор, обработку персональных данных работника в соответствии с Приложением № 1 к Правилам сбора, обработки персональных данных.

3. Внесение изменений и дополнений в следующие подзаконные акты:

1) в Правила сбора, обработки персональных данных, утвержденных Приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НҚ;

2) Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных, утвержденных Постановлением Правительства Республики Казахстан от 3 сентября 2013 года № 909;

3) Правила сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг, утвержденные Приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 406/НҚ;

4) Перечень персональных данных, необходимых и достаточных для выполнения осуществляемых задач, утвержденный Приказом Министра по инвестициям и развитию Республики Казахстан от 22 января 2018 года № 42.

4. Разработка типовой формы согласия работника на обработку его биометрических данных.

5. Разработка типовой формы запроса на получение доступа к базе персональных данных (подсистеме базы персональных данных).

6. Внесение изменений и дополнений в типовую форму Согласия на сбор и обработку персональных данных, утвержденную Правилами сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг

БИБЛИОГРАФИЯ

Нормативные правовые акты:

1. Конституция Республики Казахстан от 30 августа 1995 года.
2. Трудовой кодекс Республики Казахстан от 23 ноября 2015 года.
3. Гражданский кодекс Республики Казахстан от 27 декабря 1994 года.
4. Кодекс Республики Казахстан «Об административных правонарушениях» от 5 июля 2014 года.
5. Уголовный кодекс Республики Казахстан от 3 июля 2014 года.
6. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года.
7. Закон Республики Казахстан «О дактилоскопической и геномной регистрации» от 30 декабря 2016 года.
8. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года.
9. Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827 «Об утверждении Государственной программы Цифровой Казахстан».
10. Постановление Правительства Республики Казахстан от 3 сентября 2013 года № 909 «Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных».
11. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 406/НҚ «Об утверждении Правил сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг».
12. Приказ Министра по инвестициям и развитию Республики Казахстан от 22 января 2018 года № 42 «Об утверждении перечня персональных данных, необходимого и достаточного для выполнения осуществляемых задач».
13. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395 «Об утверждении Правил сбора, обработки персональных данных».
14. Общий регламент защиты персональных данных (GDPR) Европейского союза 2018.
15. Регламент (ЕС) 2016/679 Европейского Парламента и совета «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 / ЕС (Общие правила защиты данных)».

16. The California Consumer Privacy Act (CCPA), June 28, 2018 // https://theccpa.org/
17. Illinois Biometric Information Privacy Act, October 3, 2008 // https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57
18. ISO/IEC 2382-37 // https://www.iso.org/standard/66693.html.
19. Федеральный Закон Российской Федерации «О персональных данных» от 27 июля 2006 года.
20. Федеральный Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года.
21. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
22. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
23. Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
24. Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».
25. Постановление Правительства Российской Федерации от 13.02.2019 № 146 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных».
26. Поправки в законодательные акты Республики Казахстан по вопросам защиты персональных данных // https://legalacts.egov.kz/npa/view?id=7979084

Международные договоры:

27. Всеобщая декларация прав человека от 10 декабря 1948 года.
28. Конвенция Совета Глав Государств Содружества Независимых Государств «О правах и основных свободах человека» от 26 мая 1995 года г. Минск.
29. Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года, г. Страсбург.

Научные статьи:

30. Л.С. Асаинова «Исследование возможных экономических социальных и правовых последствий Закона Республики Казахстан «О дактилоскопической и геномной регистрации».

31. Кирилюк О.П. Международно-правовой анализ проекта Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан»
32. Лозовая О.В. «Законодательство Республики Казахстан в сфере защиты персональных данных: сравнительный анализ с правом Европейского Союза».
33. Куликпаева М.Ж. «Международно-правовые основы обеспечения права на частную жизнь в контексте развития цифровых технологий».
34. Ж.Я. Аубакирова, Э.Б. Ердеш «Цифровая трансформация: переход банков к цифровизации и инновациям»;
35. Емец Е.И. Перспективы биометрической идентификации в контексте цифровой экономики Российской Федерации;
36. А.Г. Сабанов, С. Г. Смолина Сравнительный анализ методов биометрической идентификации личности;
37. Carra Pope Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data;
38. Arun Ross Some Research Problems in Biometrics: The Future Beckons;
39. T. Ignatenko and F. M. J. Willems, Biometric Security from an Information-Theoretical Perspective, Foundations and Trends R in Communications and Information Theory, vol 7, nos 2–3, pp 135–316, 2010;
40. Mark Maguire. The birth of biometric security;
41. Stephen Mayhew. History of Biometrics;
42. Comparing privacy laws: GDPR v. CCPA;
43. Кривогин М.С. Особенности правового регулирования биометрических персональных данных;
44. Асаинова Л.С. Биометрическая аутентификация как альтернативный способ идентификации человека. Научная статья.
45. Рассолов И.М., Чубукова С.Г., Микурова И.В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // https://cyberleninka.ru/article/n/biometriya-v-kontekste-personalnyh-dannyh-i-geneticheskoy-informatsii-pravovye-problemy
46. Scope of GDPR // https://researchsupport.admin.ox.ac.uk/policy/data/scope#/;
47. MODEL REGULATION FOR DATA PRIVACY IN THE APPLICATION OF BIOMETRIC SMART CARD // https://lawjournal.ub.ac.id/index.php/law/article/view/81;
48. The impact of the GDPR and DPA 2018 on genomic healthcare and research // https://www.phgfoundation.org/documents/gdpr-and-genomic-data-report.pdf
49. Sinta dewi Rosadi. MODEL REGULATION FOR DATA PRIVACY IN THE APPLICATION OF BIOMETRIC SMART CARD //

https://www.researchgate.net/publication/315984622_MODEL_REGULATION_FOR_DATA_PRIVACY_IN_THE_APPLICATION_OF_BIOMETRIC_SMART_CARD

50. Data Protection Policy // https://www.oxfordsurfaces.com/data-protection-policy/

51. Corporate report Biometrics and forensic ethics group annual report 2019 (accessible version) // https://www.gov.uk/government/publications/biometrics-and-forensics-ethics-group-annual-report-2019/biometrics-and-forensic-ethics-group-annual-report-2019-accessible-version

52. Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? // https://www.ohchr.org/Documents/Issues/Terrorism/biometricsreport.pdf

53. Сборник практических рекомендаций ООН по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом.

Судебная практика:

54. Дело Жакашевой А.А. // https://sb.prgapp.kz/item

55. Дело Паламарь Ю.А.

56. Дело S and Marper v UK // https://justice.org.uk/s-marper-v-uk-2008/

Книги:

57. Raphaël Gellert. The googleRisk-Based Approach to Data Protection // https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198837718.001.0001/oso-9780198837718

58. David G. Hill. Data Protection: Governance, Risk Management, and Compliance // https://books.google.kz/books/about/Data_Protection.html?id=GeLaxgEACAAJ&redir_esc=y

59. Els J. Kindt. Transparency and Accountability Mechanisms for Facial Recognition // https://www.jstor.org/stable/resrep28527?Search=yes&resultItemClick=true&searchText=Biometric+Data+Protection&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DBiometric%2BData%2BProtection&ab_segments=0%2FSYC-5770%2Ftest&refreqid=fastly-default%3Ae52bd96096a0aa0874fc357f894bbb5a&seq=1#metadata_info_tab_contents

60. Астахов А. Искусство управления информационными рисками. // https://books.google.kz/books?id=1lydDQAAQBAJ&lpg=PP1&hl=ru&pg=PP1#v=onepage&q&f=false

61. The EU General Data Protection Regulation (GDPR): A Commentary // https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198826491.001.0001/isbn-9780198826491-book-part-20;

62. Hidden Biometrics. When Biometric Security Meets Biomedical Engineering;
63. Subramanian N. (2011) Biometric Authentication. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA.
64. National Research Council. 2010. Biometric Recognition: Challenges and Opportunities. Washington, DC: The National Academies Press. https://doi.org/10.17226/12720
65. Data Protection & Information Security Handbook // https://www.oxfordsu.org/pageassets/privacypolicy/Data-Protection-Handbook-V1.pdf.
Tilburg Law School. To the edge of data protection: How brain information can push the boundaries of sensitivity // http://arno.uvt.nl/show.cgi?fid=145874

Приложение 1
к Правилам сбора,
обработки
персональных данных

ТИПОВАЯ ФОРМА СОГЛАСИЯ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ
СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласие на обработку персональных данных
(информация о субъекте персональных данных)

1. Я, _____,
(ФИО)
2. ИИН _____

3. _____
(документ, удостоверяющий личность, и его номер)
4. _____
(наименование органа, выдавшего указанный документ, дата выдачи, срок действия)
5. _____
(адрес проживания)

(информация о представителе субъекта персональных данных)
*заполнить при необходимости

1. Я, _____,
(ФИО)
2. ИИН _____

3. _____
(документ, удостоверяющий личность, и его номер)
4. _____
(наименование органа, выдавшего указанный документ, и дата его выдачи)
5. _____
(адрес проживания)
6. _____
(наименование и реквизиты документа, подтверждающего полномочия представителя)

Даю согласие на сбор и обработку следующих своих персональных данных в соответствии с Перечнем персональных данных, необходимых и

достаточных для выполнения осуществляемых задач, утвержденного Приказом Министра по инвестициям и развитию Республики Казахстан от 22 января 2018 года № 42 (см. Таблица № 1):

_____

_____

(необходимо указать наименование персональных данных)

№	Наименование персональных данных
1	Фамилия
2	Имя
3	Отчество (при его наличии)
4	Сведения о смене фамилии, имени, отчества (при его наличии)
5	Транскрипция фамилии и имени
6	Данные о рождении: дата рождения; место рождения
7	Национальность
8	Пол
9	Данные документа, удостоверяющего личность: наименование документа; номер; дата выдачи; срок действия; орган, выдавший документ
10	Данные о гражданстве: гражданство (прежнее гражданство); дата приобретения гражданства Республики Казахстан; основания приобретения гражданства Республики Казахстан; дата утраты гражданства Республики Казахстан; основания утраты гражданства Республики Казахстан; дата восстановления в гражданстве Республики Казахстан; основания восстановления в гражданстве Республики Казахстан
11	Индивидуальный идентификационный номер (ИИН)
12	Портретное изображение (оцифрованная фотография)
13	Подпись
14	Адрес места жительства
15	Номера контактных телефонов
16	Адрес электронной почты
17	Юридический адрес, дата регистрации (снятия с регистрации) юридического адреса, вид деятельности
18	Сведения трудовой книжки: номер; серия; дата выдачи; записи в ней
19	Сведения о государственных и ведомственных наградах, грамотах, благодарственных письмах; Наименование или название награды; Дата и вид нормативного акта о награждении;
20	Сведения о результатах медицинских заключений
21	Сведения о социальных льготах и социальном статусе: наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса; серия, номер, дата выдачи

	документа; причина инвалидности, группа инвалидности; удостоверение, подтверждающее право на льготы пострадавшему вследствие ядерных испытаний на Семипалатинском испытательном ядерном полигоне; удостоверение, подтверждающее право на льготы пострадавшему вследствие экологического бедствия в Приаралье
22	Данные о трудовой деятельности на текущее время: полное указание должности, структурного подразделения, организации ее наименование; общий и непрерывный стаж работы; адреса и телефоны, а также реквизиты других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях
23	Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки: дата поступления в учебное заведение (отчисления из учебного заведения); серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения; наименование и местоположение образовательного учреждения; факультет или отделение, квалификация и специальность по окончании образовательного учреждения; ученая степень; ученое звание; владение иностранными языками
24	Сведение о повышении квалификации и переподготовке: серия, номер, дата выдачи документа о повышении квалификации или о переподготовке; наименование и местоположение образовательного учреждения; квалификация и специальность по окончании образовательного учреждения
25	Сведения о сдаче декларации по индивидуальному подоходному налогу и имуществу
26	Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу: серия, номер, дата выдачи (сдачи) военного билета; наименование органа, выдавшего военный билет; военно-учетная специальность; воинское звание; данные о принятии/снятии с учета; основание освобождения от воинской службы;
27	Сведения о семейном положении: состояние в браке; данные свидетельства о заключении брака; данные свидетельства о расторжении брака; фамилия, имя, отчество (при его наличии) супруги (а); данные документа, удостоверяющего личность супруги (а); степень родства; фамилии, имена, отчества (при его наличии) и даты рождения других членов семьи, иждивенцев; наличие детей (в том числе усыновленных, находящихся на попечении) и их возраст
28	Сведения о наличии (отсутствии) судимости

Таблица № 1

№	Наименование биометрических персональных данных
1	изображение лица

2	изображение сетчатки глаза
3	изображение радужки глаза
4	отпечаток ладони
5	отпечаток пальцев
6	рисунок вен
7	запись голоса
8	иные

Таблица № 2

(информация об операторе базы персональных данных)
* для оператора физического лица

1. _____,
(ФИО)
2. ИИН _____

3. _____
(документ, удостоверяющий личность, и его номер)
4. _____
(наименование органа, выдавшего указанный документ, и дата его выдачи)
5. _____
(адрес проживания)

* для оператора юридического лица
1. _____
(Наименование организации)
2. БИН _____

3. _____
(юридический адрес)
4. _____
(фактический адрес)

Цель сбора и обработки персональных данных:
_____
(цель или цели обработки персональных данных)
_____
(срок, в течение которого действует согласие)

Место и срок хранения персональных данных:
_____

(информация о собственнике базы персональных данных)
* для собственника баз персональных данных физического лица

1. _____,
(ФИО)
2. ИИН _____

3. _____
(документ, удостоверяющий личность, и его номер)
4. _____
(наименование органа, выдавшего указанный документ, и дата его выдачи)
5. _____
(адрес проживания)

* для собственника баз персональных данных юридического лица

1. _____
(Наименование организации)
2. БИН _____

3. _____
(юридический адрес)
4. _____
(фактический адрес)

В случае передачи персональных данных третьим лицам:

_____
(Цель передачи персональных данных)
_____
_____
(Перечень персональных данных, на передачу которых дается согласие субъекта персональных данных)
_____
(Срок, в течение которого действует согласие на передачу)

(информация о третьем лице)
* для физического лица
1. _____,
(ФИО)
2. ИИН _____

3. _____
(документ, удостоверяющий личность, и его номер)
4. _____
(наименование органа, выдавшего указанный документ, и дата его выдачи)
5. _____

(адрес проживания)

* для юридического лица

1. _____
(Наименование организации)
2. БИН _____

3. _____
(юридический адрес)
4. _____
(фактический адрес)

В случае трансграничной передачи персональных данных:

_____
(Наименование третьего лица, которому будут передаваться персональные данные)

_____
(Иностранные государства, которым будут передаваться персональные данные)

_____
(Цель передачи персональных данных)

_____
_____
(Перечень персональных данных, на передачу которых дается согласие субъекта персональных данных)

Порядок и основания отзыва согласия субъекта на сбор, обработку персональных данных регламентируется статьей 8 Закона Республики Казахстан «О персональных данных и их защите».

Я подтверждаю, что предоставленные мною персональные данные являются полными, актуальными и достоверными.

Я обязуюсь своевременно извещать об изменении предоставленных персональных данных.

_____
(ФИО, подпись)

_____
(данные оператора базы персональных данных, подпись)

«___» _____ 20 __ г.

Приложение 2
к Правилам сбора,
обработки
персональных данных

**ТИПОВАЯ ФОРМА ЗАПРОСА
НА ПОЛУЧЕНИЕ ДОСТУПА К БАЗЕ ПЕРСОНАЛЬНЫХ ДАННЫХ (ПОДСИСТЕМЕ БАЗЫ ПЕРСОНАЛЬНЫХ ДАННЫХ)**

_____

_____

(указать цель и основание получения доступа)

Прошу (отметить необходимое):

1. предоставить доступ к следующей базе данных персональных данных (подсистеме базы персональных данных):

_____

(наименование базе данных персональных данных (подсистеме базы персональных данных)

2. предоставить копию персональных данных:

_____

(вид персональных данных)

следующего субъекта персональных данных:

1. _____,

(ФИО)

2. ИИН _____

3. _____

(документ, удостоверяющий личность, и его номер)

4. _____

(наименование органа, выдавшего указанный документ, и дата его выдачи)

5. _____

(адрес проживания)

(Информация о лице, подающем настоящий запрос)

1. _____,

(ФИО)

2. ИИН _____

3. _____

(документ, удостоверяющий личность, и его номер)

4. _____
(наименование органа, выдавшего указанный документ, и дата его выдачи)
5. _____
(адрес проживания)

_____
(ФИО лица, подавшего запрос, подпись)

«___» _____ 20 __ г.

Приложение 3
к Правилам сбора,
обработки и хранения
биометрических данных
физических лиц для их
биометрической
аутентификации при
оказании
государственных услуг

ТИПОВАЯ ФОРМА СОГЛАСИЯ
НА СБОР И ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласие на обработку персональных данных
(информация о субъекте персональных данных)

1. Я, _____,
(ФИО)
2. ИИН _____

3. _____
(документ, удостоверяющий личность, и его номер)
4. _____
(наименование органа, выдавшего указанный документ, дата выдачи, срок действия)

В соответствии со ст. 8 Закона Республики Казахстан «О персональных данных и их защите» настоящим заявляю, что даю свое согласие некоммерческому акционерному обществу "Государственная корпорация «Правительство для граждан» на сбор и обработку биометрических данных, необходимых при оказании мне государственных услуг.

Настоящим подтверждаю, что каких-либо претензий касательно сбора и обработки персональных данных в дальнейшем иметь не буду, при условии соблюдения некоммерческим акционерным обществом «Государственная корпорация «Правительство для граждан» требований Закона и /или наших договоренностей.

Цель сбора и обработки персональных данных:

_____
(цель или цели обработки персональных данных)

_____
(срок, в течение которого действует согласие)

Место и срок хранения персональных данных:

_____

Текст настоящего согласия мной прочитан(а), дополнений, замечаний и возражений не имею.

«___» _____20___г. _____

(дата дачи согласия) (подпись)

Согласие принял(а): _____

_____

(ФИО, должность, подпись)

М.П. (проставляется штамп или печать)

* В соответствии со ст. 1 Закона Республики Казахстан от 21 мая 2013 года N94-V «О персональных данных и их защите»:

1) биометрические данные – персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность;

5) сбор персональных данных – действия, направленные на получение персональных данных;

12) обработка персональных данных – действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных.