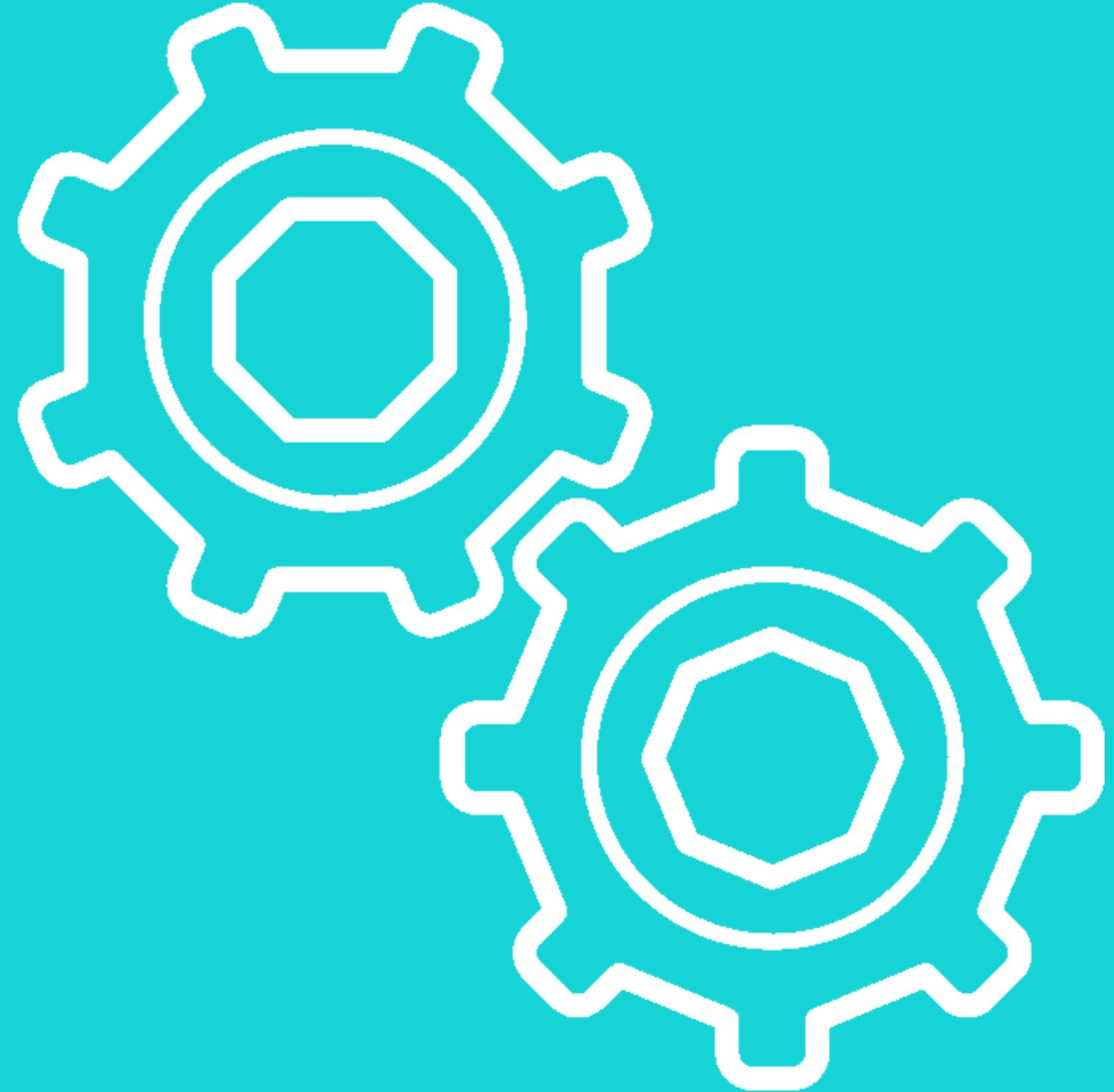


РГП на ПХВ «Национальный
научный центр развития
здравоохранения им.Салидат
Каирбековой» МЗ РК и РЦЭЗ
МЦРИАП

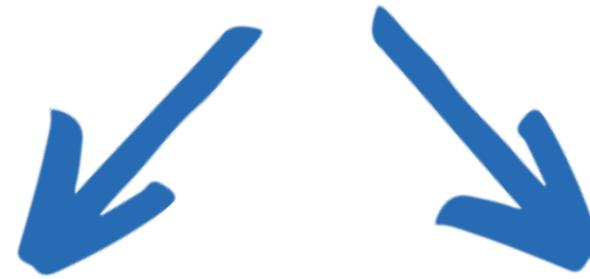
Персональные данные



Астана, 2024 г.



Персональные данные



Общедоступными персональными данными являются персональные данные или сведения, на которые в соответствии с законами Республики Казахстан не распространяются требования соблюдения конфиденциальности, доступ к которым является свободным с согласия субъекта.

Персональными данными ограниченного доступа являются персональные данные, доступ к которым ограничен законодательством Республики Казахстан.



Персональные данные

Персональные данные – это любая информация, относящаяся к конкретному человеку, позволяющая его идентифицировать напрямую или косвенно. Примеры персональных данных включают:

Имя и фамилия – очевидный идентификатор.

Контактная информация – телефонный номер, адрес электронной почты, почтовый адрес.

Идентификационные номера – паспортные данные, номера водительских удостоверений, номера социального страхования.

Финансовая информация – банковские счета, кредитные карты.

Медицинская информация – данные о здоровье, медицинские истории.

Биометрические данные – отпечатки пальцев, фотографии лица, ДНК.

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Персональные данные - сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.

Делятся на:

- общедоступные персональные данные – на них не распространяются требования соблюдения конфиденциальности, доступ к ним является свободным с согласия субъекта;

- персональные данные ограниченного доступа - доступ к ним ограничен законодательством РК.

База, содержащая персональные данные - совокупность упорядоченных персональных данных;

Субъект персональных данных - физическое лицо, к которому относятся персональные данные;

Собственник базы, содержащей персональные данные - государственный орган, физическое и (или) юридическое лицо, реализующие в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные данные;

Оператор базы, содержащей персональные данные - государственный орган, физическое и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных;

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.

Сбор персональных данных - действия, направленные на получение персональных данных;

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

Защита персональных данных - комплекс мер, в том числе правовых, организационных и технических, осуществляемых в целях, установленных Законом РК «О персональных данных их защите»;

ЭЦП — Электронная цифровая подпись

МЦРИАП — Министерство цифрового развития, инноваций и аэрокосмической промышленности

ИС — Информационная система



Статья 7. Условия сбора, обработки персональных данных и особенности сбора, обработки персональных данных из общедоступных источников

Сбор, обработка персональных данных осуществляются собственником и (или) оператором, а также третьим лицом с согласия субъекта или его законного представителя в порядке, определяемом уполномоченным органом

Распространение персональных данных в общедоступных источниках допускается при наличии согласия субъекта или его законного представителя.

Сбор и обработка персональных данных в медицинской организации

Процедура сбора и обработки персональных данных в медицинской организации должна соответствовать законодательству и обеспечивать защиту данных пациентов.

Сбор данных при первичном обращении пациента:

- Регистрация: Пациент обращается в медицинскую организацию для получения медицинских услуг.
- Заполнение анкеты: Пациент заполняет анкету, указывая основные персональные данные, такие как ФИО, дата рождения, контактная информация.
- Получение согласия: Пациент подписывает согласие на обработку персональных данных, что является обязательным требованием.
- Верификация данных: Персональные данные пациента автоматически подтягиваются из базы данных ЕГОВ КЗ, исключая 9 категорий данных, которые обрабатываются вручную.

Статья 8. Порядок дачи (отзыва) согласия субъекта на сбор, обработку персональных данных

Субъект или его законный представитель дает (отзывает) согласие на сбор, обработку персональных данных письменно, посредством государственного сервиса, негосударственного сервиса либо иным способом, позволяющим подтвердить получение согласия.

При сборе и (или) обработке персональных данных, содержащихся в объектах информатизации государственных органов и (или) государственных юридических лиц, согласие предоставляется посредством государственного сервиса.

Субъект или его законный представитель не может отозвать согласие на сбор, обработку персональных данных в случаях, если это противоречит законам Республики Казахстан, либо при наличии неисполненного обязательства.

Статья 9. Сбор, обработка персональных данных без согласия субъекта

Сбор, обработка персональных данных производится без согласия субъекта или его законного представителя в случаях:



осуществления деятельности правоохранительных органов, судов и иных уполномоченных государственных органов, которые возбуждают и рассматривают дела об административных правонарушениях, исполнительного производства



осуществления государственной статистической деятельности



использования государственными органами персональных данных для статистических целей с обязательным условием их обезличивания



реализации международных договоров, ратифицированных Республикой Казахстан

Статья 11. Конфиденциальность персональных данных

Собственники и (или) операторы, а также третьи лица, получающие доступ к персональным данным ограниченного доступа, обеспечивают их конфиденциальность путем соблюдения требований не допускать их распространения без согласия субъекта или его законного представителя либо наличия иного законного основания.

Статья 13. Изменение и дополнение персональных данных

Изменение и дополнение персональных данных осуществляются собственником и (или) оператором на основании обращения (запроса) субъекта или его законного представителя либо в иных случаях, предусмотренных законами Республики Казахстан

Статья 12. Накопление и хранение персональных данных

Накопление персональных данных производится путем сбора персональных данных, необходимых и достаточных для выполнения задач, осуществляемых собственником и (или) оператором, а также третьим лицом.

Статья 14. Использование персональных данных

Использование персональных данных должно осуществляться собственником, оператором и третьим лицом только для ранее заявленных целей их сбора.

Требования к применению ЭЦП(юр.лиц)

Если служебная ЭЦП скомпрометирована, пользователь информационной системы должен немедленно сообщить об этом своему непосредственному руководителю и сотруднику, ответственному за информационную безопасность, а также предпринять действия по отзыву и перевыпуску ЭЦП.

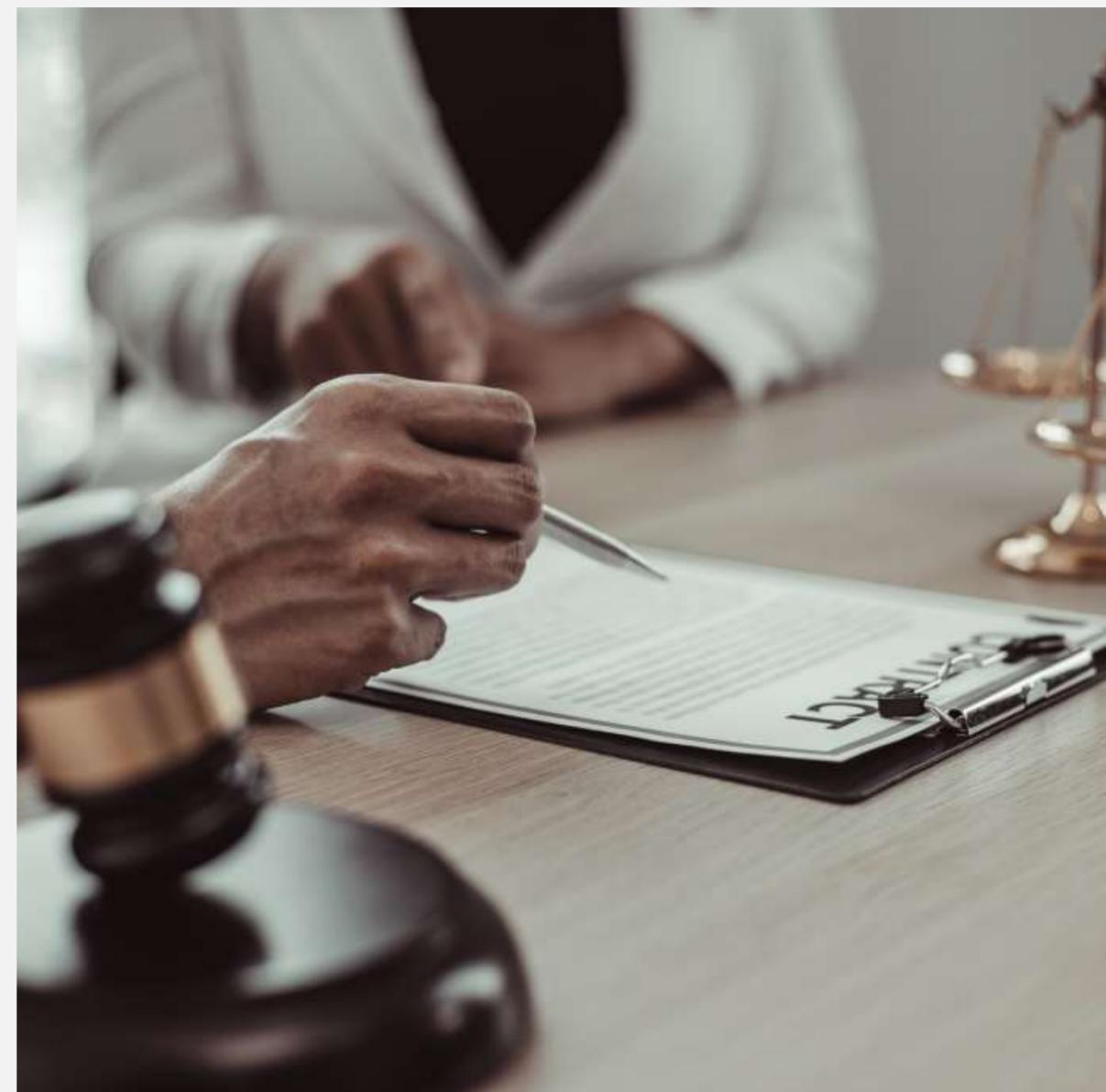
Сценарий авторизации:

- 1)Пользователь ИС выбирает авторизацию по ЭЦП и выбирает регистрационное свидетельство для подписания. Вводит пароль. ИС производит проверку регистрационного свидетельства на срок действия, проверяет статус сертификата на действительность, а также принадлежность к корневому сертификату с помощью сервисов НУЦ РК. Порядок проверки подлинности электронной цифровой подписи осуществляется в соответствии с главой 2 приказа Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи».
 - 2)При успешной проверке подписи и сертификата пользователя, ИС проводит авторизацию пользователя.
-

**О персональных данных и их защите
Закон Республики Казахстан от 21 мая 2013 года N 94-V.**

Статья 28. Надзор за применением настоящего Закона

1. Органы прокуратуры осуществляют высший надзор за соблюдением законности в сфере персональных данных и их защиты.
2. Акты прокурорского надзора, вынесенные на основании и в порядке, установленных Конституционным законом Республики Казахстан "О прокуратуре", обязательны для всех органов, организаций, должностных лиц и граждан.



СТАТЬЯ 29. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА 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.



Об административных правонарушениях

Кодекс Республики Казахстан от 5 июля 2014 года № 235-V ЗРК

Статья 641. Нарушение законодательства Республики Казахстан об информатизации

Нарушение законодательства Республики Казахстан об информатизации, совершенное в виде:

- ❖ неосуществления или ненадлежащего осуществления собственником или владельцем информационных систем, содержащих персональные данные, собственником и (или) оператором базы, содержащей персональные данные, а также третьим лицом мер по их защите;
- ❖ нарушения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности;
- ❖ утраты оригиналов технической документации на бумажных носителях;
- ❖ использование электронных информационных ресурсов, содержащих персональные данные о физических лицах, в целях причинения им имущественного и (или) морального вреда, ограничения реализации прав и свобод, гарантированных законами Республики Казахстан

влекут штраф в размере от двадцати до ста пятидесяти месячных расчетных показателей.

Примеры нарушения по персональным данным в медицинских организациях может включать следующее: Ситуация:



01

Использование слабых паролей: Медицинский сотрудник устанавливает простой или легко угадываемый пароль для доступа к электронной медицинской системе не соответствующих критериям Правил аутентификации МЗ, что может привести к несанкционированному доступу.

02

Отсутствие выхода из системы: Медицинский сотрудник не выходит из учетной записи в информационной системе после окончания работы, оставляя компьютер открытым для доступа другим лицам.

03

Передача логинов и паролей: Медицинский сотрудник делится своими учетными данными, ЭЦП с коллегами или другими сотрудниками, что нарушает политику безопасности и позволяет неавторизованным лицам получить доступ к персональным данным.

04

Отправка данных через небезопасные каналы связи: Медицинский работник отправляет медицинскую информацию пациента по незащищенным каналам связи, например, по личной электронной почте, через мессенджеры.

05

Несоответствие прав доступа: Медицинский сотрудник не проверяет и не ограничивает права доступа к медицинской информации в информационной системе, что позволяет другим сотрудникам видеть данные, к которым у них не должно быть

КЛЮЧЕВЫЕ НПА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

- [Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»;](#)
- [Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;](#)
- [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»;](#)
- [Постановление Правительства Республики Казахстан от 12 ноября 2013 года № 1214 «Об утверждении Правил определения собственником и \(или\) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач»;](#)
- [Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 21 октября 2020 года № 395/НК «Об утверждении Правил сбора, обработки персональных данных»;](#)
- [Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 30 апреля 2021 года № 156/НК «Об утверждении Правил осуществления обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах»;](#)
- [Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года № 235-V;](#)
- [Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V.](#)





**Уполномоченным
органом по защите
персональных данных
является МЦРИАП**

Спасибо за внимание !