Финансирование Европейского Союза

ИНМИР

ERKINDIK QANATY
общественный фонд

INSTITUTE FOR WAR & PEACE REPORTING
IWPR
ИНСТИТУТ РЕПОРТАЖЕЙ ВОЙНЫ И МИРА

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В НПО: ВЫЗОВЫ И РЕШЕНИЯ

POLICY BRIEF

«Эта публикация финансирована Европейским Союзом. Ее содержание является исключительной ответственностью IWPR и не обязательно отражает точку зрения Европейского Союза».

2025

Содержание

ОБ АВТОРЕ

Куралай Каракулова
Юрист, Магистр юридических наук.
Сертифицированный глобальный тренер
по правам человека, правам женщин (WLP USA).
Эксперт по гендерному равенству
Правовой эксперт Программы развития ООН в Казахстане
Член Евразийской палаты юристов г.Алматы.

ОБ ОБЩЕСТВЕННОМ ФОНДЕ «ЕРКІНДІК ҚАНАТЫ»

Общественный Фонд «Еркіндік Қанаты» был создан 6 марта 2015 года.

Фонд является правозащитной организацией открытого типа, аккумулировавшей в себе опыт и ценности, приобретенные в процессе формирования активной гражданской позиции организаторов и волонтеров фонда.

Основными направлениями работы фонда являются общественная защита и продвижение прав и свобод, образовательные программы, проведение исследований, в том числе посредством мониторинга, а также участие в законотворческой деятельности.

ОБ IWPR

IWPR (Институт репортажей войны и мира) усиливает голос местных сообществ, помогая им добиваться перемен в странах, переживающих конфликты, кризисы и переходные периоды. Там, где распространяется язык вражды и пропаганда, а журналисты и гражданские активисты подвергаются атакам, IWPR продвигает достоверную информацию и способствует общественным дискуссиям, которые действительно имеют значение. В условиях, когда новые формы дезинформации способствуют расколу в обществе, растут цифровые угрозы и учащаются нападения на журналистов, миссия IWPR по поддержке местных голосов становится особенно важной. Основная задача организации — укрепление потока достоверной и объективной информации, позволяющей журналистам и гражданскому обществу информировать, обучать и мобилизовать сообщества. IWPR помогает обществам находить собственные решения, усиливая их потенциал в сфере журналистики и гражданской активности, а также поддерживая борьбу за подотчётность, свободу слова и права человека.

О ЕВРОПЕИСКОМ СОЮЗЕ

Европейский Союз – это экономический и политический союз 27 европейских стран. Он основан на ценностях уважения человеческого достоинства, свободы, демократии, равенства, верховенства закона и уважения прав человека, в том числе прав лиц, принадлежащих к меньшинствам. Он действует на глобальном уровне с целью продвижения устойчивого развития общества, окружающей среды и экономики во благо каждого.

Данная Аналитическая записка подготовлена в рамках Проекта "Гражданское общество за Казахстан (CS4K)", реализуемого Институтом по освещению войны и мира (IWPR) в партнерстве с Институтом национальных и международных инициатив развития (ИНМИР) при финансовой поддержке Европейского союза.

Проект направлен на продвижение фундаментальных свобод и прав в Казахстане посредством усилий гражданского общества.

ВВЕДЕНИЕ

В настоящее время современный мир по праву уже называют цифровым миром. При этом внедрение цифровых технологий происходит с использованием информации.

Объем информации, передаваемая через интернет, стремительно растет. Это и регистрация в онлайн—сервисах, использование социальных сетей и мобильных приложений и всё это сопровождается передачей личной информации человека.

Но не многие задумываются о том, что, сообщая о себе информацию, сознательно или неосознанно предоставляют другим людям свои персональные данные.

Ведь информация о человеке — это чувствительные личные данные, что делает её уязвимой для мошенничества, угроз, краж и негативного влияния на обладателя информации.

Между тем, необходимо отметить, что личная информация, персональные данные напрямую связаны с обеспечением основных прав и свобод человека, в частности — **права на неприкосновенность частной жизни**, **личную тайну** *и* **достоинство личности**.

Впервые это право было регламентировано в **Всеобщей декларации прав человека** *в статье 12 – «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств.»*[1]

1 Всеобщая декларация прав человека, Принята резолюцией 217A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года

В дальнейшем это право было закреплено в **Международном пакте о гражданских и политических правах** *в статье 17 – «Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию.»*[2]

Персональные личные данные — это часть частной жизни человека. Их незаконный сбор, распространение может привести к нарушению **прав человека**.

Поэтому в настоящее время защита персональных данных является актуальной повесткой не только на международном, но и на национальном уровне. Казахстан не является исключением и на законодательном уровне разрабатывает основные направления государственной политики в сфере персональных данных и их защиты.

Ключевыми аспектами защиты персональных данных в Казахстане являются:

1) установление четких правовых гарантий по защите персональных данных;

2) обеспечение защиты прав субъектов персональных данных;

3) внедрение информационных и технических решений для защиты данных, а также развитие кибербезопасности.

4) принятие мер по привлечению к ответственности лиц, допустивших нарушения законодательства о персональных данных и их защите.

Государства, организации и общества в целом несут ответственность за то, чтобы цифровые технологии и механизмы сбора, обработки персональных данных не нарушали фундаментальные свободы граждан.

2 Международный пакт о гражданских и политических правах, Принят резолюцией 2200 А (XX1) Генеральной Ассамблеи от 16 декабря 1966 года

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Международное регулирование защиты персональных данных является важным аспектом, особенно в условиях глобализации и роста объемов данных. Разные страны устанавливают свои правила, положения однако сформировались **международные документы и принципы**, которые объединяют эти усилия и в конечном итоге обеспечивают единый подход к защите частной жизни.

И таким основным международным документом стал **Регламент № 2016/679 Европейского Парламента и Совета Европейского Союза от 27 апреля 2016 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных** *(GDPR — General Data Protection Regulation)*. Регламент называют главным международным стандартом, принятый в Европейском союзе, который вступил в силу 25 мая 2018 года.

Целью данного Регламента является защита физических лиц в отношении обработки персональных данных и правила свободного обращения персональных данных. А также защита основных прав и свобод физических лиц и, в особенности, права на защиту персональных данных.

Важным моментом является, что Регламент представляет собой унифицированные для ЕС правила, т.е. единые нормы касающиеся обработки персональных данных.

Более того, Регламент закрепил универсальные принципы обработки персональных данных:

Статья 5. Принципы обработки персональных данных

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

b. собираются для конкретных, ясных и законных целей, и их дальнейшая обработка не осуществляется несовместимым с этими целями способом;

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»).

e. хранятся в форме, допускающей идентификацию субъектов данных, не дольше, чем это необходимо в целях, для которых обрабатываются персональные данные;

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 соответствующих технических или организационных мер («целостность и конфиденциальность»).

Эти принципы обладают экстерриториальным регулированием, это означает, что все государственные органы, организации, компании собирающие, обрабатывающие и хранящие персональные данные физических лиц должны соответствовать закрепленным принципам *Генерального регламента ЕС*.

Ключевая особенность данного регламента в том, что в нем очень широко закреплено понятие **«персональные данные»**.

Статья 4 Определения

«**персональные данные**» – любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, фамилия, идентификационный номер, данные о местоположении, онлайн—идентификатор или один или несколько характерных для указанного лица физических, физиологических, генетических, духовных, экономических, культурных факторов или ссылаясь на факторы социальной идентичности;

Кроме того, Регламент содержит обязательное требование по получению согласия на использование и обработку данных, а также право на удаление данных и назначение специалиста по защите персональных данных в организациях.

Следующим международным документом является *«Конвенция о защите физических лиц при автоматизированной обработке персональных данных»* принятый членами Совета Европы 28 января 1981 году один из первых документов по данному вопросу.

«Целью настоящей Конвенции является обеспечение на территории каждой из Сторон уважения прав и основных свобод каждого человека независимо от его гражданства или места жительства и в особенности его права на неприкосновенность личной сферы в связи с автоматической обработкой касающихся его персональных данных («защита данных»).[3]

Также следует отметить, что подобные документы по защите персональных данных приняты в странах Азиатско—Тихоокеанского региона, в Канаде, Бразилии и в некоторых странах Африки.

Все эти документы поддерживают добровольные принципы приватности и фокусируются на балансе между защитой прав и свобод и развитием бизнеса.

Организация Объединенных Наций (ООН) признает важность защиты персональных данных и разработала ряд рекомендаций и принципов, направленных на обеспечение конфиденциальности и безопасности личной информации.

3 «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» принятый членами Совета Европы 28 января 1981 году.

Одним из первых документов была Резолюция Генеральной Ассамблеей 68/167 от 18 декабря 2013 года. Право на неприкосновенность личной жизни в цифровой век.

Главным посылом данной резолюции ко всем государствам это уважать и защищать право на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации. А также принимать меры по соблюдению прав субъектов личной информации, предотвращать нарушения, привести национальное законодательство в соответствии с международными обязательствами по международному праву прав человека.

Резолюции, политики ООН, регулирующие вопросы защиты персональных данных

— Резолюция Генеральной Ассамблеей 69/166 от 18 декабря 2014 год Право на неприкосновенность частной жизни в цифровую эпоху

— Политика по защите персональных данных лиц, подпадающих под компетенцию УВКБ ООН, 2015 год

— Принципы защиты персональных данных и конфиденциальности (принят Комитетом высокого уровня ООН по управлению (КВУУ) на 36—м заседании 11 октября 2018 год

— Резолюция Совета по правам человека 48/4 от 7 октября 2021 год

Право на неприкосновенность частной жизни в цифровую эпоху

— Общая политика в отношении персональных данных и конфиденциальности (GDPP) УВКБ ООН, 2022 год

Кроме того, ООН учредил институт Специального докладчика по вопросу о праве на неприкосновенность частной жизни в марте 2015 года.
Мандат специального докладчика уполномочивает его поощрять и защищать право на конфиденциальность путем:

Обзора государственной политики и законов о перехвате цифровых сообщений и сборе персональных данных

Выявление действий, нарушающих конфиденциальность без веских на то оснований

Помощь правительствам в разработке передовых методов обеспечения глобального наблюдения в соответствии с принципом верховенства закона

Формулирование обязанностей частного сектора по соблюдению прав человека

Помощь в обеспечении соответствия национальных процедур и законов международным обязательствам в области прав человека.

Государственные органы, коммерческие организации и организации гражданского общества должны следовать этим международным стандартам, чтобы быть открытыми, безопасными и легитимными в глазах партнёров и граждан.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КАЗАХСТАНЕ

Согласно статье 18 Конституции Республики Казахстан *«Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства.»*[4]

Указанная конституционная норма свидетельствует о том, что согласно Конституции, наиболее защищённой в государстве информацией, наряду с информацией, составляющей государственную тайну, являются сведения о частной жизни человека.

(Комментарии к ст.10 Гражданского процессуального кодекса Республики Казахстан).

«Частная жизнь — это сфера жизнедеятельности одного отдельного человека, которая дорога только ему, поэтому вмешательство со стороны общества, государства без согласия на то самого лица недопустимо. Личная тайна, являясь частью частной жизни, предполагает наличие сведений, которые лицо хранит в секрете. К ним можно отнести сведения, касающиеся здоровья, подробности интимной жизни и др. Семейная тайна предполагает наличие сведений, скрываемых от посторонних близкими родственниками, т.е. членами семьи. К ним относятся тайна усыновления и другие взаимоотношения в семье. Учитывая большую значимость для лица его частной жизни, законодатель признает ее неприкосновенной, и ограждает от любого незаконного вмешательства.»

Поскольку персональные данные включают сведения о частной жизни человека, то необходимо обеспечить право на неприкосновенность частной жизни, право на личную и семейную тайну применительно к обработке персональных данных и их защите.

В дальнейшем конституционная норма была регламентирована через принятие специального закона. Так 21 мая 2013 года был принят **Закон Республики Казахстан «О персональных данных и их защите»** (далее — Закон).

Согласно статье 2 Закона *Целью настоящего Закона является обеспечение защиты прав и свобод человека и гражданина при сборе и обработке его персональных данных.*[5]

4 Конституция Республики Казахстан, принята на республиканском референдуме 30 августа 1995 года
5 Закон Республики Казахстан «О персональных данных и их защите» принят 21 мая 2013 года № 94—V

Важным аспектом Закона является закрепление принципов защиты персональных данных. Так в соответствии со статьей 5 Закона Сбор, обработка и защита персональных данных осуществляются в соответствии со следующими 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.

Особо хотелось отметить, что **субъектом персональных данных является только физическое лицо,** к которому относятся персональные данные, т. е. носитель персональных данных.

Согласно определению, принятого Законом — **персональные данные *это сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе*.**

В данном случае персональные данные — это любая информация, так или иначе относящаяся к субъекту персональных данных, включающая как прямые, так и косвенные признаки, позволяющие идентифицировать человека. На практике к персональным данным относятся фамилия, имя, отчество, дата рождения, гражданство, образование, семейное положение, адрес проживания и другие сведения о субъекте.

Вместе с тем персональные данные по доступности делятся на общедоступные и ограниченного доступа.

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. Согласно п.3 *Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных* Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих возможность несанкционированного, в том числе случайного, до-

ступа к персональным данным при их сборе и обработке, результатом которого могут стать уничтожение, изменение, блокирование, копирование, несанкционированное предоставление третьим лицам, несанкционированное распространение персональных данных, а также иные неправомерные действия.

В соответствии со статьей 8 Закона Согласие на сбор и обработку персональных данных включает:

п.4 статья 8 Закона «О персональных данных и их защите»

1) наименование (фамилию, имя, отчество (если оно указано в документе, удостоверяющем личность), бизнес—идентификационный номер (индивидуальный идентификационный номер) оператора;

2) фамилию, имя, отчество (если оно указано в документе, удостоверяющем личность) субъекта;

3) срок или период, в течение которого действует согласие на сбор, обработку персональных данных;

4) сведения о возможности оператора или ее отсутствии передавать персональные данные третьим лицам;

5) сведения о наличии либо отсутствии трансграничной передачи персональных данных в процессе их обработки;

6) сведения о распространении персональных данных в общедоступных источниках;

7) перечень собираемых данных, связанных с субъектом;

8) иные сведения, определяемые собственником и (или) оператором.

Особо хотелось обратить внимание на подпункт 8 иные сведения, определяемые собственником и (или) оператором. Данная норма диспозитивная, что в свою очередь создает риски по сбору различных сведений, которые могут быть использованы для манипуляций в отношении обладателя персональных данных.

Между тем, стоит отметить, что в статье 14 Закона «О персональных данных и их защите» закреплено, что *Использование персональных данных должно осуществляться собственником, оператором и третьим лицом только для ранее заявленных целей их сбора.*

То есть сбор объема (количества) сведений/данных о субъекте должно быть исключительно на основании заявленных целей, в противном случае сбор сведений без цели будет считаться незаконным.

Одним из основных требований для осуществления сбора и обработки персональных данных является обеспечение их защиты.

Согласно п.11 статьи 1 Закона ***защита персональных данных – это комплекс мер, в том числе правовых, организационных и технических****, осуществляемых в целях, установленных настоящим Законом.*

Принятая норма указывает на то, что при работе с персональными данными необходимо принять соответствующие меры по защите персональных данных.

В этих целях в Законе приняты правовые основы деятельности, связанные со сбором, обработкой и защитой персональных данных, которая включает следующие правовые, организационные меры:

- ✓ Защита персональных данных
- ✓ Сбор персональных данных
- ✓ Накопление персональных данных
- ✓ Хранение персональных данных
- ✓ Обработка персональных данных
- ✓ Изменение персональных данных
- ✓ Дополнение персональных данных
- ✓ Использование персональных данных
- ✓ Распространение персональных данных
- ✓ Обезличивание персональных данных
- ✓ Блокирование персональных данных
- ✓ Уничтожение персональных данных

Особо следует отметить, что в Законе закреплены права и обязанности субъектов, которые в той или иной мере ответственны по работе с защитой персональных данных.

Такими субъектами выступают:

1) **физическое лицо**, к которому относятся персональные данные;
2) **собственник базы** в лице государственного органа, физического и (или) юридического лица, реализующие право владения, пользования и распоряжения базой, содержащей персональные данные;
3) **оператор базы** в лице государственного органа, физического и (или) юридического лица, осуществляющие сбор, обработку и защиту персональных данных;

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

В рассматриваемом контексте общественные организации являются операторами базы, осуществляющие сбор, обработку и защиту персональных данных.

В Законе закреплены компетенции государственных органов, которые реализуют государственное регулирование в сфере персональных данных при этом определен уполномоченный орган.

Государственным уполномоченным органом в данном случае выступает **Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (Комитет информационной безопасности).**

Статья 27–1 Компетенция уполномоченного органа

1) формирует и реализует государственную политику в сфере персональных данных и их защиты;

1—1) осуществляет государственный контроль за соблюдением законодательства РК о персональных данных и их защите;

2) разрабатывает порядок осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных;

2—1) разрабатывает правила определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач;

2—2) определяет порядок определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач;

2—3) определяет порядок осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных;

3) рассматривает обращения субъекта или его законного представителя о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение;

4) принимает меры по привлечению лиц, допустивших нарушения законодательства РК о персональных данных и их защите, к ответственности, установленной законами РК;

5) требует от собственника и (или) оператора, а также третьего лица уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

6) осуществляет меры, направленные на совершенствование защиты прав субъектов;

6—1) создает консультативный по вопросам персональных данных и их защиты, а также определяет порядок его формирования и деятельности;

6—2) направляет оператору информационно—коммуникационной инфраструктуры «электронного правительства» информацию о нарушении безопасности персональных данных, влекущем риск нарушения прав и законных интересов субъектов;

7) утверждает правила сбора, обработки персональных данных;

7—1) утверждает правила осуществления обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах, по согласованию с Комитетом национальной безопасности РК;

7—2) утверждает правила функционирования государственного сервиса контроля доступа к персональным данным;

7—3) согласовывает интеграцию негосударственных объектов информатизации с объектами информатизации государственных органов и (или) государственных юридических лиц, при которой осуществляется передача персональных данных и (или) предоставляется доступ к персональным данным;

7—4) утверждает правила интеграции с государственным сервисом контроля доступа к персональным данным;

8) осуществляет иные полномочия, предусмотренные настоящим Законом, иными законами РК, актами Президента РК и Правительства РК.

Хотелось обратить внимание на важную норму в Законе это статья 27 – 2, которая предусматривает государственный контроль за соблюдением законодательства Республики Казахстан о персональных данных и их защите осуществляемая в форме внеплановой проверки в соответствии с Предпринимательским кодексом.

Согласно данной нормы государственный уполномоченный орган вправе проводить контроль организаций в том числе и некоммерческих на предмет соблюдения Закона «О персональных данных и их защите».

Для сведения: статистические данные

С начала 2024 года на сегодняшний день проведено 11 внеплановых проверок и возбуждено и рассмотрено 23 административных дел по нарушению требований законодательства Республики Казахстан в сфере персональных данных и их защиты, по итогу которых по различным частям статьей 79 и 641 КоАП РК привлечено к ответственности 4 физических лица и 25 юридических и должностных лиц, наложены штрафы на общую сумму 4 910 360 тенге.

Источник: Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности РК

При этом насколько динамика привлечения к административной ответственности меняется не представляется возможным, так как уполномоченный орган не публикует такие сведения на своем сайте.

Между тем, мы можем просмотреть некоторую динамику в открытых источниках на просторах интернета. Так согласно данным от finprom.kz в январе–июле текущего года в Казахстане зарегистрировали 65 административных нарушений закона о персональных данных и их защите — на 75,7% больше, чем в аналогичном периоде 2023 года. При этом рассмотрено было 61 дело против всего 23 годом ранее. Постановления о привлечении к административной ответственности вынесли в отношении 61 человека — в 2,9 раза больше, чем в январе–июле прошлого года. За нарушения законодательства в секторе наложили штрафы на 10,1 млн тенге, взыскали 8,1 млн тенге.[6]

Следующий открытый источник Liter.kz передает что в 2024 году в сфере защиты персональных данных проведено 60 внеплановых проверок и административных разбирательств на общую сумму 12 млн 153 тыс. 455 тенге. Это значительно больше, чем в 2023 году, когда было зарегистрировано 38 таких проверок.

Также данный источник цитирует председателя Комитета по информационной безопасности МЦРИАП РК Руслана Абдикаликова, который озвучил следующие

6 Источник: https://kapital.kz/tehnology/128514/v—rk—rastet—chislo—pravonarusheniy—svyazannykh—s—zashchitoy—personal—nykh—dannykh.html

данные: “В сфере обеспечения информационной безопасности за год проведено 210 внеплановых проверок и административных дел без выезда на место на общую сумму 7 млн 817 тыс. 810 тенге. В области электронного документа и ЭЦП рассмотрено 10 административных дел на сумму 304 тыс. 519 тенге”.[7]

Таким образом, следует отметить, что увеличилось количество административных дел за нарушение закона о персональных данных.

Такая тенденция указывает что необходимо усилить работу по безопасности персональных данных и проводить мероприятия по повышению уровня цифровой грамотности не только граждан, но и представителей юридических лиц.

Надо отдать должное на сегодняшний день сфера персональных данных находится под строгим контролем государства. Так согласно Приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 29 апреля 2022 года № 144/НҚ утверждены Правила функционирования государственного сервиса контроля доступа к персональным данным.

Государственный сервис контроля доступа к персональным данным *(далее – Сервис КДП)* предназначен для предоставления доступа к персональным данным после получения соответствующего согласия со стороны гражданина, посредством отправки SMS—сообщения от 1414 с запросом на доступ к персональным данным или иным путем субъекта персональных данных.
Согласно Закону Сервис КДП является обязательным в случае взаимодействия с объектами информатизации государственных органов, содержащих персональные данные.

Так, на сегодняшний день с Сервисом КДП интегрированы 81 информационных систем: из них 35 государственные информационные системы, 9 информационных систем квазигосударственного сектора, 37 частные информационные системы.

Сервис КДП позволяет гражданам контролировать использование их персональных данных, содержащихся в государственных базах данных, путем дачи разрешения или отказа в доступе к ним.

7 https://liter.kz/v—kazakhstane—proveli—proverki—na—12—mln—tenge—v—sfere—zashchity—personalnykh—dannykh—1742455826/

Нормативно—правовые акты для регламентации функционирования и интеграции с Сервисом КДП:

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 апреля 2022 года № 144/НҚ «Об утверждении Правил функционирования государственного сервиса контроля доступа к персональным данным» (Зарегистрирован в Министерстве юстиции Республики Казахстан 7 мая 2022 года № 27963);
Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 8 июля 2022 года № 236/НҚ «Об утверждении Правил интеграции с государственным сервисом контроля доступа к персональным данным» (Зарегистрирован в Министерстве юстиции Республики Казахстан 13 июля 2022 года № 28786).

Государство продолжает работу по пристальному вниманию соблюдению закона о защите персональных данных.

Подтверждением является то, что 28 марта 2023 года утверждена Концепция цифровой трансформации, развития отрасли информационных технологий и кибербезопасности на 2023–2029 годы.(Утверждена Постановлением Правительства Республики Казахстан от 28 марта 2023 года № 269.)

В рамках Концепции в целевом индикаторе 10 «Доля государственных информационных систем, подключенных к сервису контроля доступа к персональным данным» предусмотрены 2 мероприятия, по первому мероприятию срок исполнения запланирован на декабрь 2025 года, по второму мероприятию реализация исполнения предусмотрена на ежегодной основе.

По первому мероприятию предусмотрено присоединение к Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера (Конвенция принята в 1981 году Советом Европы известную как «Конвенция 108»).

По второму мероприятию предусматривается Ежегодный мониторинг государственных информационных систем, подлежащих к интеграции с системой контроля доступа к персональным данным.

Это первый международный договор, посвященный праву лиц на защиту их персональных данных. Данная Конвенция даст право расследовать нарушения прав наших граждан в сфере защиты персональных данных, совершаемых операторами стран, присоединившихся к Конвенции.

Данная Конвенция даст право расследовать нарушения прав наших граждан в сфере защиты персональных данных, совершаемых операторами стран, присоединившихся к Конвенции.

В связи с этим необходимо отметить, что государство проводит соответствующие меры по комплексному анализу всех необходимых процедур и законотворческих работ по имплементации нормы Конвенции и GDPR.Согласно статье 29 Закона установлена ответственность за нарушение законодательства о персональных данных и их защите.

Полномочиями по привлечению лиц к административной ответственности за нарушение требований законодательства о персональных данных и их защите, электронном документе и электронной цифровой подписи наделен Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности РК.

Так Комитет по информационной безопасности рассматривает дела об административном правонарушении в указанных сферах, предусмотренные статьями 79, 640 и 641 КоАП РК. Выше приведена статистика по привлечению к административной ответственности.

КоАП РК от 5 июля 2014 года

Статья 79. Нарушение законодательства Республики Казахстан о персональных данных и их защите

1. Незаконные сбор и (или) обработка персональных данных, если эти деяния не содержат признаков уголовно наказуемого деяния, -

влекут штраф на физических лиц в размере тридцати, на должностных лиц, частных нотариусов, частных судебных исполнителей, адвокатов, юридических консультантов, субъектов малого предпринимательства или некоммерческие организации - в размере шестидесяти месячных расчетных показателей.

2. Те же деяния, совершенные собственником, оператором или третьим лицом с использованием своего служебного положения, если эти действия не влекут установленную законом уголовную ответственность -

влекут штраф на физических лиц в размере ста, на должностных лиц, субъектов малого предпринимательства или некоммерческие организации - в размере двухсот месячных расчетных показателей.

3. Несоблюдение собственником, оператором или третьим лицом мер по защите персональных данных, если это деяние не содержит признаков уголовно наказуемого деяния, -

влечет штраф на физических лиц в размере ста пятидесяти, на должностных лиц, субъектов малого предпринимательства или некоммерческие организации - в размере трехсот месячных расчетных показателей.

4. Деяние, предусмотренное частью третьей настоящей статьи, повлекшее утерю, незаконный сбор и (или) обработку персональных данных, если эти деяния не влекут установленную законом уголовную ответственность, -

влечет штраф на физических лиц в размере двухсот, на должностных лиц, субъектов малого предпринимательства или некоммерческие организации - в размере семисот пятидесяти месячных расчетных показателей.

Для защиты прав субъектов персональных данных предусмотрена статья 30 Закона Действия (бездействие) субъекта, собственника и (или) оператора, а также третьего лица при сборе, обработке и защите персональных данных могут быть обжалованы в порядке, установленном законами Республики Казахстан.

С принятием Закона **«О персональных данных и их защите»** в Республике Казахстан началось создание специальных законодательных основ по защите персональных данных.

Ниже приводится список некоторых кодексов, законов, нормативных правовых актов, регулирующих деятельность по защите персональных данных.

№п\п	Наименование нормативных правовых актов	
1.	Трудовой кодекс	от 23 ноября 2015 года № 414—V
2.	Социальный кодекс	от 20 апреля 2023 года № 224—VII ЗРК
3.	Кодекс «О здоровье народа и системе здравоохранения»	от 7 июля 2020 года № 360—VI
4.	Предпринимательский кодекс	от 29 октября 2015 года № 375—V
5.	Конституционный закон «О прокуратуре»	от 5 ноября 2022 года № 155—VII
6.	Закон ««Об онлайн—платформах и онлайн—рекламе»	от 10 июля 2023 года № 18—VIII ЗРК.
7.	Закон «О государственной статистике»	от 19 марта 2010 года № 257—IV

8.	Закон «Об информатизации»	от 24 ноября 2015 года № 418—V
9.	Закон «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций»	от 4 июля 2003 года № 474—II
10.	Правила сбора, обработки персональных данных	Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности от 21 октября 2020г № 395/НҚ
11.	Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных	Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности от 12 июня 2023г № 179/НҚ
12.	Правила определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач	Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности от 21 июня 2023г № 199/НҚ
13.	Правила осуществления обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах	Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности от 30 апреля 2021г № 156/НҚ
14.	Перечень персональных данных, необходимого и достаточного для выполнения осуществляемых задач Агентством по стратегическому планированию и реформам, Бюро национальной статистики	Приказ Председателя Агентства по стратегическому планированию и реформам от 24 июня 2022г №3
15.	Правила осуществления уведомления субъектов персональных данных о нарушении безопасности персональных данных	Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности от 9 августа 2024г № 481/НҚ

16.	О некоторых вопросах консультативного совета по вопросам персональных данных и их защиты	Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности от 12 апреля 2022г № 118/НҚ
17.	Правила функционирования государственного сервиса контроля доступа к персональным данным	Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности от 29 апреля 2022г № 144/НҚ
18.	Проверочного листа за соблюдением законодательства о персональных данных и их защите в отношении собственников и (или) операторов, а также третьих лиц	Совместный приказ Министра цифрового развития, инноваций и аэрокосмической промышленности от 19 марта 2024г № 149/НҚ и приказ Зам Премьер–Министра – Министра нацэкономики от 19 марта 2024г № 12
19.	Правил интеграции с государственным сервисом контроля доступа к персональным данным	Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности от 8 июля 2022г № 236/НҚ
20.	Хранение и передача персональных данных ограниченного доступа осуществляются с использованием средств криптографической защиты информации, имеющих параметры не ниже третьего уровня безопасности	Стандарт РК СТРК1073–2007 «Средства криптографической защиты информации. Общие технические требования».

Таким образом, с учетом глобальных тенденций и вызовов в области безопасности данных, Казахстан стремится создать эффективную систему защиты, соответствующую международным принципам.

АНАЛИЗ РЕЗУЛЬТАТОВ ОПРОСА ПО ВОПРОСАМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕННЫХ ОРГАНИЗАЦИЯХ КАЗАХСТАНА

В период с февраля по март 2025 года Общественный Фонд «Еркіндік қанаты» провел опрос среди некоммерческих организаций (далее – НКО) по вопросу защиты персональных данных в общественных организациях Казахстана.

Целью данного онлайн—опроса было изучение практик защиты персональных данных в некоммерческих организациях Казахстана.

При проведении исследования были использованы два вида методик:

1. Онлайн анкетирование
2. Фокус группы

В онлайн анкетировании приняли участие представители 117 некоммерческих организаций из различных регионов Казахстана.

При этом следует отметить, что по состоянию на апрель 2023 года количество зарегистрированных НПО составляет – 23 335. (Источник: Комитет информации Министерства информации и культуры Республики Казахстан).[8]

Для анализа результатов анкетирования были отобраны ответы, которые имеют государственную регистрацию в уполномоченном государственном органе.

Анкета состоит из 33—х вопросов и поделена на разделы. Для анализа были отобраны ответы на более актуальные вопросы, раскрывающие цель исследования.

РЕЗУЛЬТАТЫ АНКЕТИРОВАНИЯ

1.1 В первом разделе анкеты была отражена основная административно—организационная информация об организации.

В опросе приняли участие некоммерческие организации из 17 регионов Казахстана. Наибольшее количество ответов поступило из города Алматы — 27 (23,5%), города Астаны — 17 (14,8%), Костанайской области — 8 (7,0%),

8 https://www.gov.kz/memleket/entities/inf/activities/142?lang=ru

Восточно—Казахстанской области — 8 (7,0%), Павлодарской области — 7 (6,1%) и Туркестанской области — 7 (6,1%).

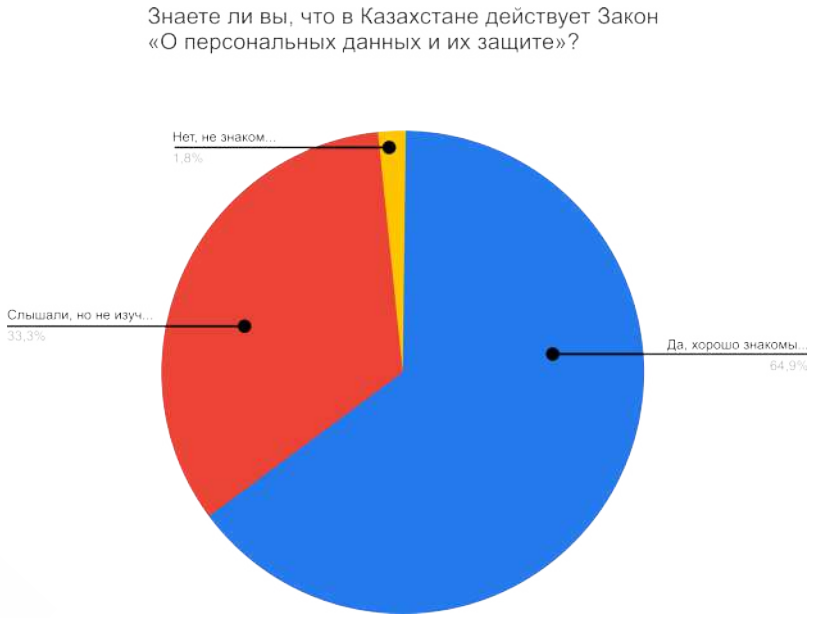
По количеству штата работников/волонтеров в организации показало, что большинство организаций имеют менее 10 работников или волонтёров: от 5 до 10 человек — 38,9%, менее 5 человек — 36,3%.

Насколько организация вела активную деятельность через реализацию определенных проектов за 2024 год выяснилось, что более половины организаций (55,8%) реализовали от 1 до 5 проектов, тогда как 14,2% — не реализовали ни одного проекта. И только 9,7% провели более 10 проектов.

Опрос показал, что наибольшее количество опрошенных организаций (35,2%) работают в сфере прав человека, далее следует сфера образование (16,4%), и на третьем месте сфера экология, где работают (11,4%).

2.2. Второй раздел анкетирования был посвящен вопросам осведомленности о защите персональных данных

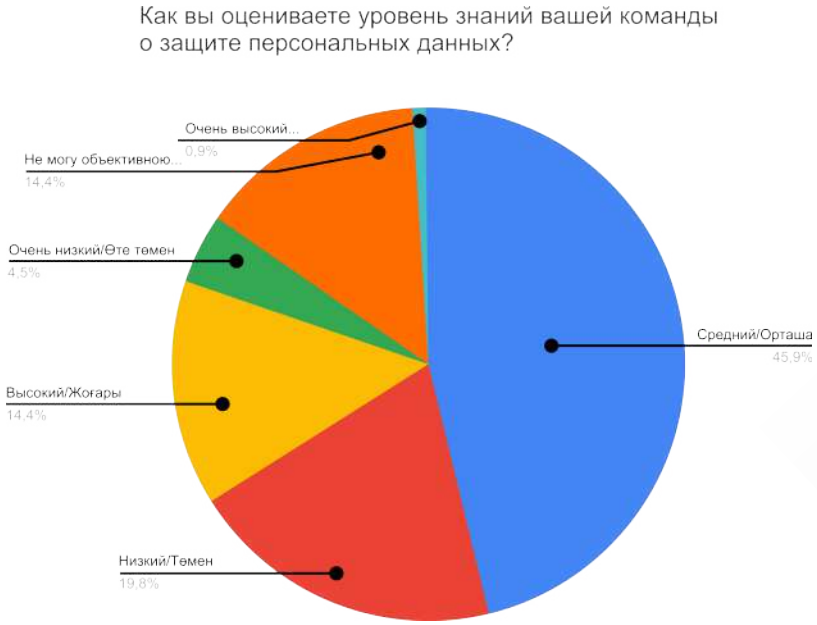
На вопрос анкеты Знаете ли вы Закон Республики Казахстан «О персональных данных и их защите 64,9% респондентов ответили что хорошо знакомы с Законом «О персональных данных и их защите». Однако, 33,3% респондентов ответили, что слышали о законе, но не изучали его.



Вместе с тем 52,3% респондентов правильно указали Комитет по информационной безопасности при МЦРИАП как уполномоченный орган.

Но при этом треть респондентов (28,8%) затруднились ответить на вопрос какой государственный орган отвечает за регулирование данной сферы. Остальная часть респондентов выбрали неверные варианты ответов или не знали ответа вовсе.

Далее, следует отметить, что при оценке уровня осведомленности о защите персональных данных непосредственно командой организации показывает среднюю осведомленность – 45,9%. Респонденты считают знания своих коллег средними, и только 14,4% оценивают уровень осведомленности как высокие. Низкий уровень осведомленности отметили 19,8% респондентов.



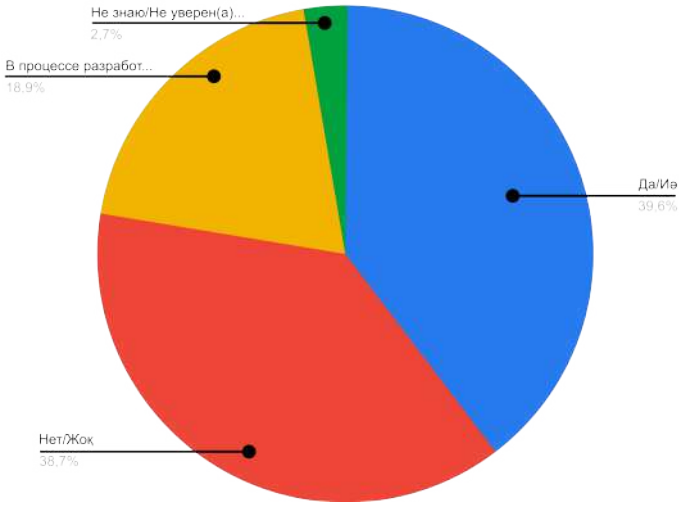
3.1. Третий раздел опроса касается текущей практики управления персональными данными в организации.

Так на вопрос имеет ли организация регламент/положение по сбору, обработке, хранению персональных данных только 39,6% организаций указали что имеют внутренние политики и/или регламенты по обработке данных, а 38,7% вовсе не имеют таких документов. При этом в процессе разработки внутренних документов находится у 18,9% организаций.

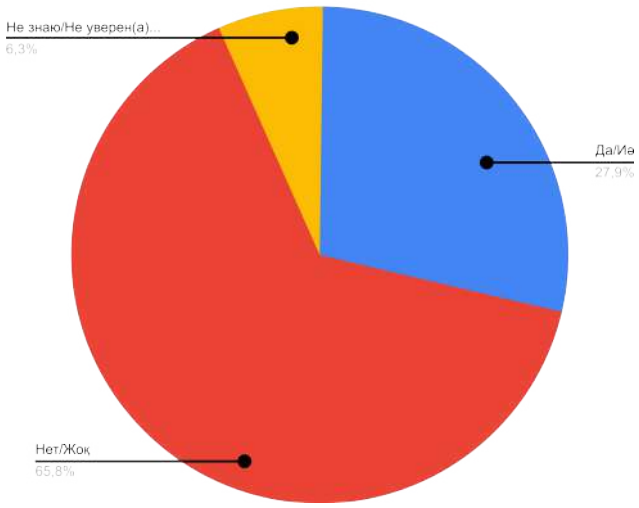
Кроме того, лишь 27,9% респондентов указали, что в их организации назначено ответственное лицо за обработку и защиту персональных данных.

И к сожалению 65,8 % опрошенных не назначили ответственное лицо.

Есть ли у вашей организации политика/ регламент/положение по сбору, хранению и обработкеперсональных данных

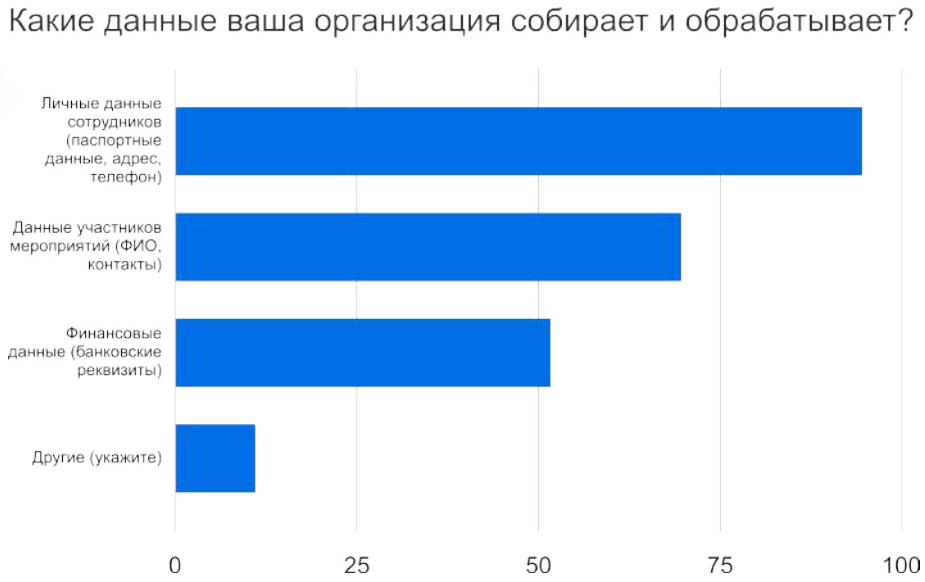


Назначен ли в вашей организации ответственный за обработку и защиту персональных данных?

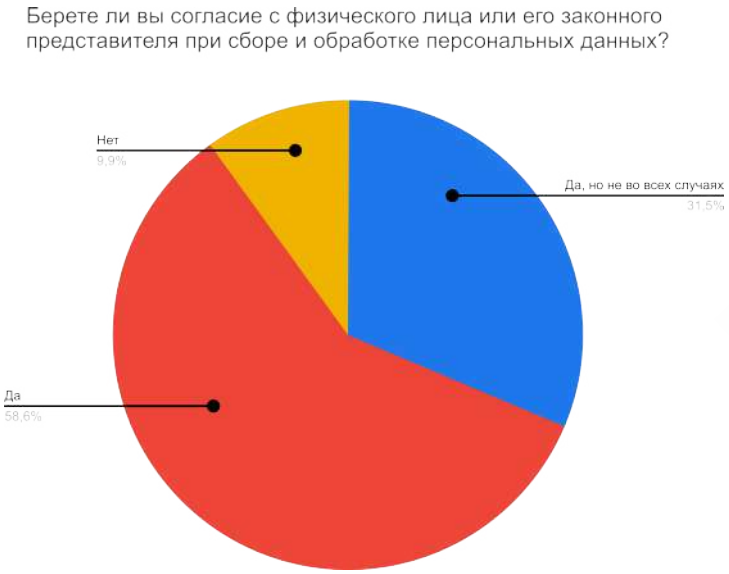


На вопрос какие данные или типы документов организация собирает выяснилось, что большинство организаций собирают и обрабатывают личные данные работников (паспортные данные, адрес, телефон). Далее сбор данных участников мероприятий, в частности ФИО, контакты. И на третьем месте — финансовые данные (банковские реквизиты).

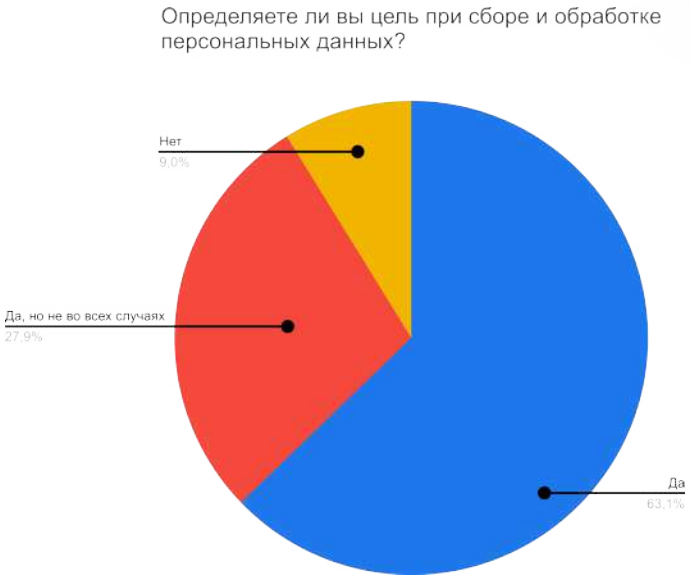
В категории «Другие» несколько респондентов указали такие данные как медицинская информация, документы других бенефициаров, информация о социальных программах. Но в то же время опрос показал, что имеются некоторые организации, которые отметили, что вообще не собирают персональные данные.



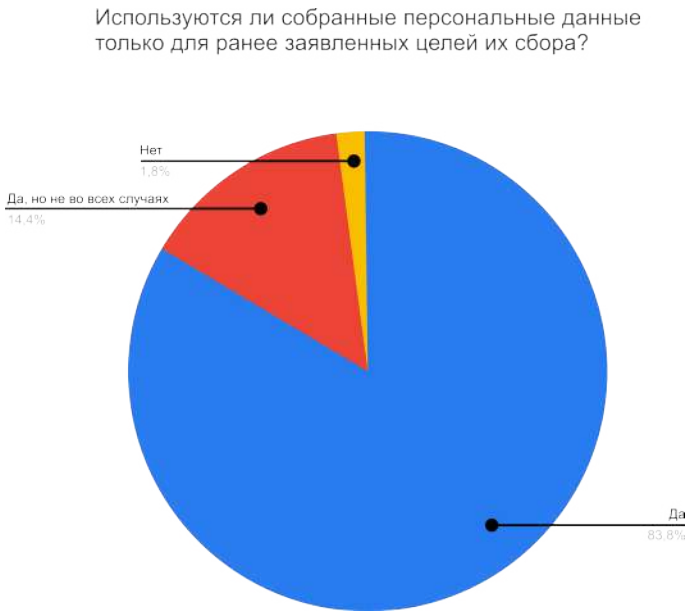
На вопрос берет ли организация согласие от физического лица или его законного представителя при сборе, обработке персональных данных 58,6% респондентов указали, что отбирают согласие на обработку данных, но 31,5% респондентов делают это не во всех случаях. И только 9,9% не берут согласие.



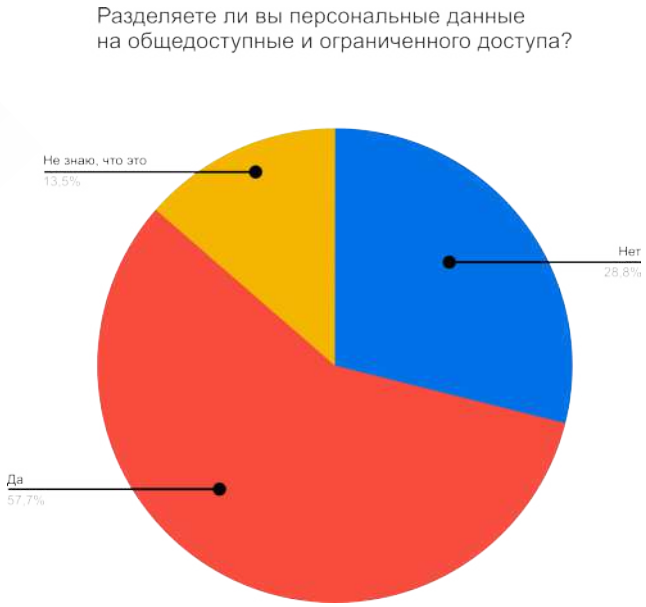
Вместе с тем, ситуация с определением целей сбора, обработки персональных данных показало, что половина респондентов (63,1%) четко формулирует цель при сборе данных. Но 27,9% ответивших не во всех случаях определяют цель.



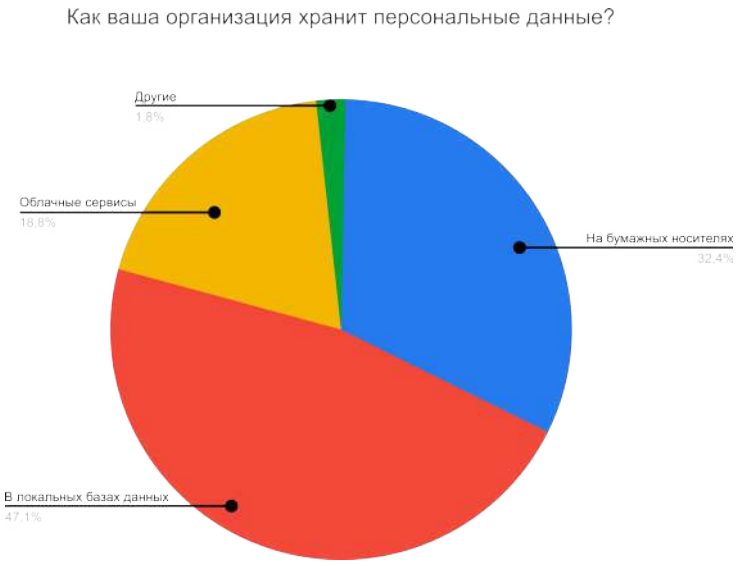
Высокую оценку 83,8%. показывает ответ на вопрос используются ли собранные персональные данные только для ранее заявленных целей. Лишь 14,4% не во всех случаях используют данные по ранее заявленной цели.



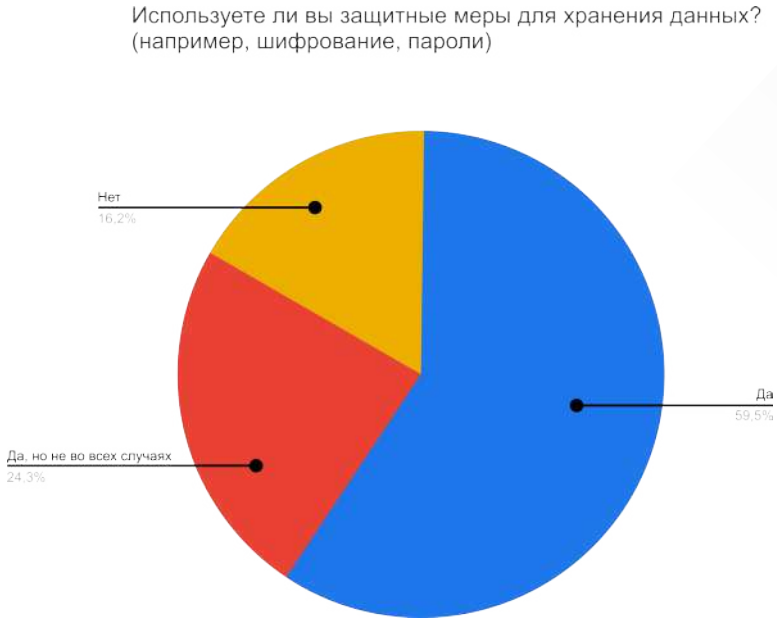
На вопрос разделяет ли организация персональные данные на общедоступные и ограниченного доступа выяснилось, что 57,7% респондентов разграничивают данные. А 28,8% респондентов не разграничивают. Но следует отметить, что 13,5% отвечавших не знают, что это.



Опрос показал, что хранение персональных данных происходит следующим образом большинство организаций, хранят данные в локальных базах (47,1%), на бумажных носителях хранят (32,4%), и на облачных сервисах хранят 18,8% респондентов.



Насколько применяются защитные меры по хранению персональных данных ответы распределились следующим образом 59,5% респондентов заявили, что применяют защитные меры (в виде пароли, шифрование), но почти четверть организаций (24,3%) делают это нерегулярно, а 16,2% вовсе не используют никаких мер защиты.



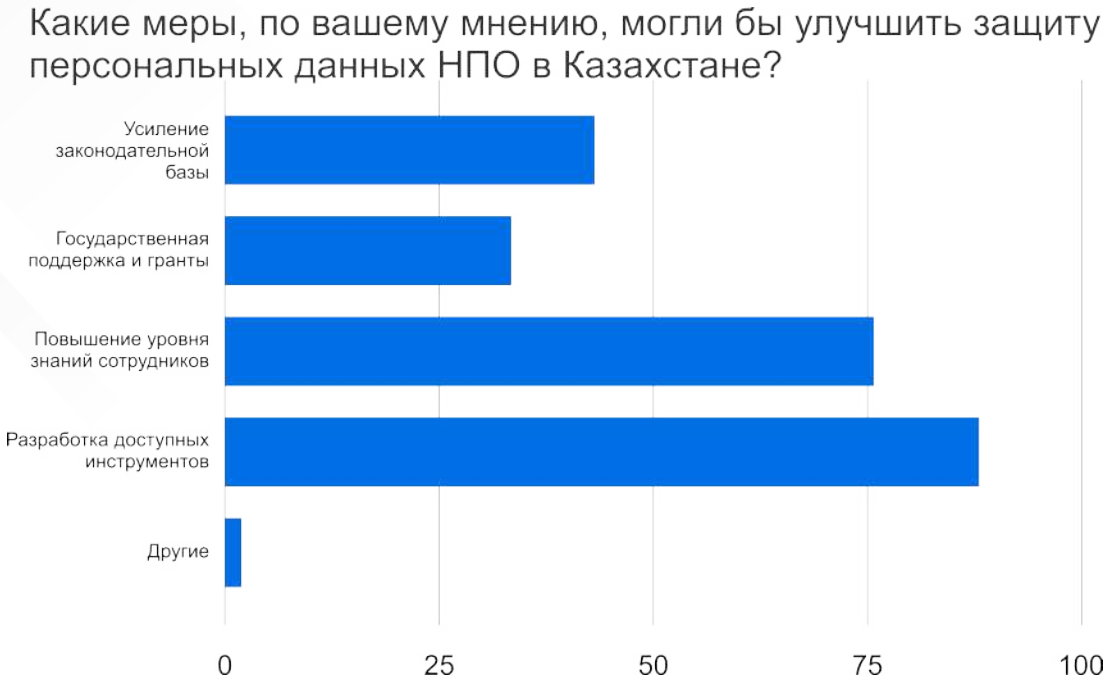
Важно отметить, что в данном опросе 10 организаций сообщили о случаях возможной утечки персональных данных. Среди указанных инцидентов были отмечены кражи жёстких дисков, компьютера, использование программы «Пегасус», публикация персональных данных на иностранных интернет–ресурсах, а также утечка пароля от электронной почты.

4.1 Четвертый раздел анкетирования был посвящен тому с какими трудностями, и потребностями сталкиваются в организации, а также какие меры нужны для защиты персональных данных в общественных организаций.

Так на вопрос с какими трудностями сталкивается организация по защите персональных данных результаты ответов показывают, что основными трудностями, с которыми сталкиваются общественные организации в вопросах, защиты персональных данных являются:

- ✓ нехватка знаний и навыков у сотрудников – 54,9%
- ✓ ограниченные финансовые ресурсы для внедрения мер защиты – 49,6%
- ✓ нехватка технических инструментов, таких как программное обеспечение или оборудование – 46,9%
- ✓ проблемы с доступом к юридической или технической помощи – 36,3%.

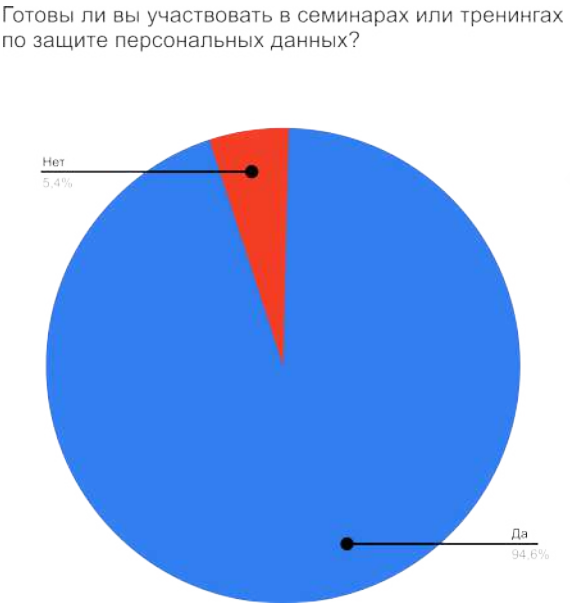
- ✓ непонимание законодательных требований — 33,6%
- ✓ отсутствие заинтересованных или ответственных сотрудников — 29,2%



На вопрос какие меры могли бы улучшить защиту персональных данных НПО в Казахстане были предложены следующие меры:

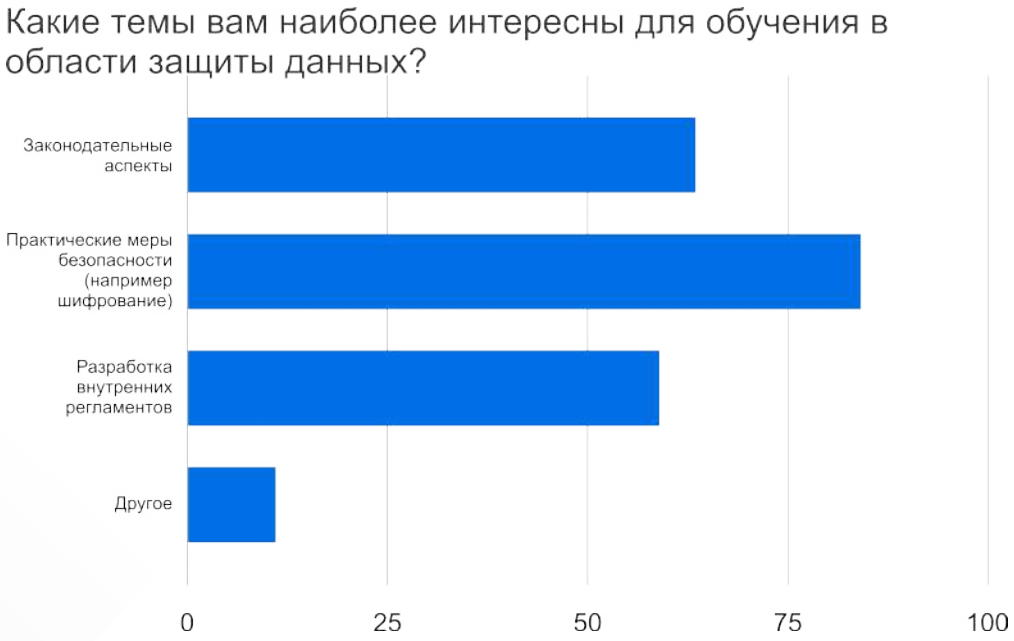
- ✓ Большинство респондентов предложили разработку доступных инструментов для защиты персональных данных.
- ✓ Следом идет повышение уровня знаний работников организаций.
- ✓ Усиление законодательной базы.
- ✓ Государственная поддержка и гранты.

Особо необходимо отметить, что имеется потребность в получении знаний по данной теме об этом, свидетельствуют ответы респондентов. Так на вопрос «Готовы ли вы участвовать в семинарах или тренингах по защите персональных данных» 94,6% ответили — да.



При этом при ответах обозначились темы наиболее интересные для обучения в области защиты персональных данных, такие как:

1. Практические меры безопасности (например шифрование).
2. Законодательные аспекты.
3. Разработка внутренних регламентов.



АНАЛИЗ РЕЗУЛЬТАТОВ ФОКУС—ГРУПП ПО ВОПРОСАМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕННЫХ ОРГАНИЗАЦИЯХ КАЗАХСТАНА

Помимо анкетирования в рамках исследования были проведены 5 фокус—групп (2 были проведены оффлайн в Астане и 3 фокус группы онлайн).

В фокус группах участвовали представители 29 общественных организаций из 9 регионов Казахстана: Астана, Алматы, Туркестанская область, Усть—Каменогорск, Павлодар, Уральск, Семей, Атырау и Тараз.

Целью проведенных фокус групп являлось провести более глубокий анализ практик и сложностей, связанных с обработкой персональных данных, а также проверка и уточнение результатов онлайн—опроса.

В ходе обсуждений большинство выводов, полученных через анкетирование, были подтверждены, а также дополнены контекстом, который показывает подходы к персональным данным, применяемые некоммерческими организациями на практике, а также кейсы из работы.

Также, как и в опросе, большинство участников фокус—групп были правозащитники, но также были организации, чья деятельность была направлена на исследования, творческие проекты, экологию и другие сферы.
Для анализа применяется тематический анализ выявляя определенные схожести или различия в работе разных организаций.

РЕЗУЛЬТАТЫ ФОКУС ГРУППЫ

1. Политики по работе с персональными данными

Как показали результаты как опроса, так и фокус—групп, у большинства общественных организаций отсутствуют отдельные, формализованные политики или регламенты, посвященные работе с персональными данными.

При этом, в ходе обсуждений стало ясно, что отдельные элементы таких политик всё же присутствуют в других внутренних документах организаций. Например, в ряде случаев заключаются соглашения о неразглашении персональных данных при оформлении договоров с сотрудниками, а также используются согласия на обработку данных при их сборе. У некоторых организаций положения, касающиеся работы с персональными данными, прописаны как часть внутренних процедур, например, в документах по работе с бенефициарами или при организации мероприятий.

Цитаты из ответов респондентов

«*Раньше мы запрашивали копию удостоверения личности для хранения в документации. Поскольку законодательство поменялось, мы перестали это делать. И мы сейчас просто просим людей либо написать нам данные удостоверения личности, либо самостоятельно заполнить это в договоре. То есть мы уже не прикладываем к договорам никакие копии удостоверений.*» *(Алматы)*

«*Большинство в Казахстане некоммерческих организаций достаточно компактные [...] со штатом там, от двух даже от одного человека бывают. В среднем, штаб некоммерческих организаций 3—5 человек. Тут важно понимать а для кого пишутся эти политики. То есть политики уместны тогда, когда существуют какие—то серьезные бизнес—процессы и коммуникации в рамках рабочих отношений. И в контексте большинства организаций некоммерческого сектора уместность большинства политик во многих случаях видятся необязательными. Например, нас заставляют делать политику управления кадрами. Какое управление кадров, если кадры составляют директор, бухгалтер и координатор? Но какое управление кадров, если все это может регулироваться должностными инструкциями, которые являются приложением к индивидуальным трудовым договорам?*» *(Алматы)*

«*Поскольку мы обязаны хранить всю первичную финансовую документацию для налоговых целей на протяжении 10 лет, для пенсионных целей пожизненно, все что касается штата сотрудников, мы естественно архивируем это все. Архивация происходит согласно определенным правилам и требованиям. Все это хранится в офисе под тремя замками. Вот в электронном виде первичная документация у нас хранится только в том случае, если мы направляем какой—то скан финансовой отчетности нашим донорам. И это все тоже архивируется. в формате облачного хранения, но хранится ровно столько, сколько требуется по требованию, собственно, самих доноров. Это может быть 3, 5, 10 лет, стандартные сроки по хранению.*» *(Усть—Каменогорск).*

Среди тех, кто внедрил полноценные политики, можно выделить две основные группы. Первая — это организации, которые **приняли такие документы в рамках требований доноров** (в основном иностранных). Вторая — те, кто **разработали и внедрили политику после прохождения обучающих программ** и использует её в повседневной практике, осознавая её значимость.

При этом представители обеих групп отмечают, что на практике соблюдение всех положений документа крайне сложно. Основные причины: нехватка времени, человеческих ресурсов и ограниченные организационные возможности, что особенно характерно для небольших общественных организаций с ограниченным бюджетом направленных только на реализацию проектов.

2. Отсутствие системного подхода

Из предыдущей части вытекает вторая ключевая особенность практик по работе с персональными данными в общественных организациях — отсутствие системного подхода, связанное в первую очередь с ограниченностью ресурсов и сложности понимания законодательных требований. Практически все организации предпринимают те или иные действия для защиты данных. К примеру, используют защищённые места хранения (например, металлические сейфы), удаляют персональные данные после окончания проектов, применяют двухфакторную аутентификацию, сложные пароли, а также включают приписки согласия при сборе данных через онлайн—формы.

Однако эти меры носят несистемный характер и часто реализуются без единой стратегии или координации. В условиях работы общественных организаций, когда несколько человек в организации могут совмещать разные функции и основной фокус ставится на реализацию деятельности проектов, вопросы защиты данных не получают должного приоритета.

Более того, несмотря на ознакомление с Законом «О персональных данных и их защите», респонденты отмечают нехватку понимания практического применения правовых требований и нехватку разъяснения от уполномоченных органов. Организациям не хватает адаптированных разъяснений, инструкций и примеров, которые бы учитывали специфику их деятельности и реальные возможности реализации норм на практике.

3. Работа с донорами

“У нас каждый раз возникает вот этот вопрос передачи данных донору, потому что мы не можем гарантировать сохранность этих данных у донора, будь это зарубежная организация, международная или государственная организация [...] А требования идут вплоть до копии документов.” (Усть—Каменогорск).

Одним из важных аспектов, поднятых в ходе фокус—групп, стала тема взаимодействия с донорами, особенно в контексте передачи персональных данных бенефициаров. Специфика работы некоммерческих организаций тесно связана с работой с донорами как международными, так и государственными и обязательной отчетностью перед ними.

В ряде случаев для подтверждения реализации проекта, оказанных услуг и освоения бюджета доноры запрашивают не только общедоступные данные такие как ФИО, но и чувствительную информацию, включая копии документов, справки о диагнозах, сведения о социальных статусах и другие.

Организации могут обеспечивать защиту данных внутри своей структуры. Однако после передачи данных донору, контроль за дальнейшим использованием и хранением становится невозможным.

Особо остро проблема стоит при работе с государственными грантами, регулируемые Центром поддержки гражданских инициатив (ЦПГИ). Как отмечают респонденты, в текстах грантовых соглашений нередко прямо указывается требование передачи персональных данных участников проектов, включая их ФИО, контактные данные, иные сведения. Для общественных организаций это создает конфликт между юридическим обязательством передать данные и ответственностью за их защиту.

Более того, в ходе обсуждений всплыли случаи, когда через несколько лет после завершения проекта бенефициарам звонили представители государственных органов с вопросами об их участии в проектах, что может указывать на длительное хранение данных в структурах, не подконтрольных некоммерческим организациям.

4.Ответственность государственных органов

В ходе фокус—групп проявилось устойчивое ощущение тревожности среди представителей некоммерческих организаций, связанное с работой с персональными данными. Кроме нехватки знаний и ресурсов, это также связано с недоверием со стороны бенефициаров и потенциальной угрозы со стороны государственных структур, включая взлом внутренних систем и проверок.

Многие организации отмечают, что всё больше бенефициаров боятся предоставлять персональные данные в контексте участившихся случаев кибермошенничества. Особенно это отмечается в проектах, где работа ведётся с пожилыми группами.

Параллельно существует опасение, что государственные органы могут получить доступ к внутренним данным организаций. Участники делились случаями, когда подобные вмешательства уже происходили. Так, респондентка из города Тараз описывала ситуацию, когда эксперт, получивший гонорар получил звонки из полиции с вопросами об их деятельности. Никакой передачи данных со стороны организации не было, и источником такой информации, по мнению участницы, могли быть только государственные или банковские системы.

Цитата из ответа респондента

«Всем бенефициарам, кто получал от организации гонорары, поступили звонки от третьих лиц, от сотрудников полиции, от банка, от КНБ даже было. И то, что выше уже говорили, что первая угроза, это от государства. Я хочу это подтвердить на своем личном опыте, так как кроме меня вообще никто не владеет информацией. Я сама веду бухгалтерию организации, то есть слив был только с моего отчета в налоговый комитет, либо же с банка, от менеджеров, которые видят состояние счетов и суммы на счетах.» (Тараз)

Это формирует ощущение незащищенности даже в тех случаях, когда организация соблюдает все нормы закона. В результате, тема защиты данных воспринимается не только как технический и юридический вопрос, но и как фактор безопасности самой организации.

Важно отметить, что без законодательных оснований государственные органы не вправе требовать персональные данные работников организаций.

Сбор и обработка персональных данных осуществляются только с согласия субъекта или его законного представителя, за исключением отдельных случаев. При этом сбор и обработка персональных данных в том числе и их использование должны проводиться только в рамках установленных целях оператором. Вместе с тем, оператор должен составить четкий и конкретный перечень необходимых персональных данных, которые необходимы для реализации установленной цели.

Те отдельные случаи когда не требуется согласие субъекта или его законного представителя на сбор, обработку персональных данных закреплены в статье 9 Закона «О персональных данных и их защите».

В данном описываемом ответе респондента это в случае осуществления деятельности правоохранительных органов, судов и иных уполномоченных государственных органов, которые возбуждают и рассматривают дела об административных правонарушениях, исполнительного производства. Но следует отметить, что данные дела должны быть в производстве, проходит расследование, а также в связи с проведением проверки.

5. Потребности организаций и рекомендации для устойчивой работы с персональными данными

Анализ опросов и фокус—групп показал, что общественные организации Казахстана сталкиваются не только с ресурсными ограничениями, но и с отсутствием системной, понятной и доступной поддержки в вопросах работы

с персональными данными. Эти ограничения касаются как внутренних возможностей организаций, так и регулирования.

Одним из наиболее выраженных потребностей организаций стало доступное обучение по законодательству, включая новые подзаконные акты, а также консультации и сопровождение по правоприменению.

Представители общественной организации подчеркивают, что одного ознакомления с законом недостаточно, нужен «перевод» норм на язык практики: понятные материалы, визуальные методички, инструкции и памятки, особенно рассчитанные на неюристов. К примеру, онлайн—курсы, мини—лекции с пошаговыми действиями, которые всегда доступны.

Важным предложением стало создание инструментов автоматизации, например, Telegram—бота, который генерирует шаблоны согласий, политик и напоминает о необходимости удаления данных.

Многие подчеркивают, что в условиях нехватки ресурсов, как финансовых, так и кадровых, общественные организации не могут позволить себе юристов или выделенные департаменты. Поэтому особенно актуальна идея аутсорсинга или типовых решений для сектора. Существующая практика в бизнесе, где есть готовые продукты, могла бы быть адаптирована для некоммерческого сектора.

Отдельный блок рекомендаций касается законодательной и институциональной среды. Участники фокус группы подчеркивают, что:

- Необходимо уменьшить санкции, особенно в отношении некоммерческих организаций, и избегать репрессивных подходов.
- Важно не только наказывать, но и поощрять соблюдение норм, бонусами, приоритетами в конкурсах и признанием.
- Законы нужно сделать четкими, однозначными, не подлежащими произвольной интерпретации. Сейчас они трактуются по—разному, что создает юридическую неопределенность.
- Необходимо, чтобы при разработке норм участвовали независимые эксперты и представители общественных организаций, а не только государственные органы.
- Государству следует демонстрировать пример: при постоянных утечках из госорганов (что признается публично) доверие к требованиям теряется.
- Роль государства должна быть не только регулирующей, но и поддерживающей. Общественные организации хотят видеть реальную реакцию государства, прозрачные каналы коммуникации, централизованные ресурсы, а также четкие алгоритмы обжалования и возможность получения оперативной помощи, включая горячую линию и доступную юридическую поддержку.

ВЫЗОВЫ И РИСКИ, СВЯЗАННЫЕ С ЗАЩИТОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕННЫХ ОРГАНИЗАЦИЯХ

Результаты анкетирования и опроса выявили практические схожие проблемы, риски в сфере защиты персональных данных. Многие отвечавшие говорили о важности защиты персональных данных, но были и другие, которые не до конца понимали смысл Закона о защите персональных данных и их защите.

В целом опрос носил общий характер, поскольку в рамках исследования ставилась задача понять, как обстоят дела с безопасностью защитой персональных данных в общественных организациях.

Вместе с тем выяснилось, что представители общественных организаций в большинстве знакомы с Законом «О персональных данных и их защите» и заинтересованы в повышении уровня осведомленности в этих вопросах.

На основании проведенного опроса в качестве основных вызовов и угроз в области персональных данных предлагается выделить следующие:

1. **Инновационные технологические изменения**: Быстрый рост технологий, в том числе облачных решений и мобильных приложений, и другие инновации создают новые требования для обработки и защиты персональных данных.

2. **Часто меняющиеся законы, правила**: Вносимые изменения, дополнения в нормативные правовые акты требуют периодического обновления внутренних политик и процедур по защите персональных данных.

3. **Отсутствие или недостаток знаний и навыков**: Субъекты персональных данных как правило не осознают, кому, зачем и в каком объеме они передают свои персональные данные. Это ведет к пробелам в области правового обеспечения защиты персональных данных, к трудностям в соблюдении действующего законодательства со стороны организаций. Необходимо обеспечить персонал достаточными знаниями в области защиты персональных данных. Зачастую работники не осознают рисков, связанных с обработкой персональных данных.

4. **Ограниченные ресурсы**: Общественные организации не имеют достаточных финансовых средств для внедрения современных систем безопасности, привлечения отдельного специалиста по защите персональных данных, а также обучения работников.

5. **Отсутствие самоконтроля:** Субъекты персональных данных не отслеживают дальнейшие действия в отношении их персональных данных. Что в свою очередь минимизировало бы риски по неправомерному использованию данных.

6. Случайное или преднамеренное копирование документов, разглашение информации вследствие случайного или преднамеренного выведения на печать.

Кроме того, предлагается выделить некоторые риски, которые могут нанести вред как обладателю персональных данных, так и общественным организациям:

1. Утечка данных. Неправильное обращение с данными может привести к их утечке, что может нанести серьёзный ущерб как организациям, так и лицам, чьи данные были раскрыты. Каналами утечек информации являются: съемные носители информации, электронная почта, бумажные документы, стационарный компьютер, мобильное оборудование.

2. Неправомерный доступ к базам данных, связан с уязвимостью программного сервиса и обеспечения, а также человеческий фактор.

3. Внешние угрозы (кибератаки, фишинг, вредоносное программное обеспечение и др.). В частности, общественные организации могут стать мишенью для хакеров, особенно если они не имеют соответствующих мер защиты.

4. Внутренние угрозы (ошибки работников, недостаток информированности незнание законодательства в данной области и т.д.).

5. Недостаток контроля: Отсутствие постоянного контроля за обновлениями программного обеспечения и системы, используемые для хранения и обработки данных, могут оказаться неудовлетворительными или устаревшими, что повышает риск утечек и атак.

6. Мошенничество или неправомерное использование персональных данных. Всякого рода манипуляции, обманные пути вхождения в доверие могут спровоцировать мошеннические действия.

7. Нарушение законодательства: В случае невыполнения норм и требований по защите данных может привести к значительным штрафам. Данный риск негативно отразится на деятельности общественной организации вплоть до приостановления.

8. Низкий уровень цифровой грамотности. Среди населения еще имеется значительное количество граждан, которые не владеют навыками работы с данными и технологиями. И это может отразиться в эффективном использовании данных, а также при сборе, обработке и хранении данных.

В связи с этим необходима системная работа по преодолению этих вызовов и рисков, требуется комплексный подход. Начиная с обучения персонала, улучшения институциональной системы внутри организации, развитие политики и стратегии управления персональными данными и активное участие всех заинтересованных лиц.

РЕКОМЕНДАЦИИ

В целях соблюдения прав человека, защиты персональных данных, а также во избежания рисков, нарушений конфиденциальности, нарушений норм законодательства в области защиты персональных данных необходимо принять соответствующие меры.

Проведенный опрос продемонстрировал что представители общественных организаций имеют слабое представление какие нужно принимать меры, политику, документы в организации.

В связи с этим **рекомендуется:**

1. Общественным организациям разработать в организации практические инструменты в виде следующих типов документов:

1. Политика защиты и обработки персональных данных. Данный документ должен быть разработан на основании норм Закона, а также со спецификой или видом деятельности организации.

2. Положение о персональных данных работников. В основе документа должны учитываться нормы Трудового кодекса Республики Казахстан, включая право на ознакомление с текстом Положения Работника.

3. Положение о порядке ведения личных дел работников, правилах обработки, хранения и передачи персональных данных работников, содержащихся в личных делах

4. Разработка и внедрение политики конфиденциальности. Документ должен четко и конкретно определять какую информацию собирает организация, как она будет использоваться и кто будет иметь к ней доступ.

5. Форма согласия на обработку персональных данных, основываясь на Законе «О персональных данных и их защите»

6. Разработка Программы Обучения работников. Проводить регулярные тренинги по вопросам защиты персональных данных для повышения осведомленности о лучших практиках и способах предотвращения утечек информации.

7. Разработка Программы шифрования защиты, хранения данных. Привлечь специалиста для разработки программы.

8. Акты работодателя для проведения регулярного аудита и проверок с привлечением специалиста по выявлению уязвимостей и их своевременного устранения.

9. **Положение о** х**ранении персональных данных**. Включить срок хранения персональных данных и их удаление в связи с исчерпанием цели сбора и хранения

10. Акты работодателя по соблюдению законодательства в сфере защиты персональныхданных.Изучатьнациональноеимеждународноезаконодательство о защите персональных данных. Минимизировать риски, связанные с их утечкой или неправомерным использованием.

11. Анализуязвимостей. Регулярноепроведениетестированиянапроникновение и анализ уязвимостей в системах обработки данных.

12. Информирование. Создание информационных материалов (буклеты, памятки, внутренние рассылки) о принципах обработки и защиты персональных данных.

13. Регулярный анализ текущих практик позволит организациям соблюдать законодательные требования, повысить доверие клиентов и партнеров.

14. Приказ о назначении специалиста ответственного лица за работу с персональными данными.

Лишь немногие участники опроса смогли ответить на вопросы, связанные с государственным регулированием защиты персональных данных и в частности, на вопрос какой государственный орган является уполномоченным органом в этой сфере.

Вместе с тем, учитывая, что в профильном Законе имеются пробелы в регулировании определенных общественных отношений предлагаются следующие рекомендации:

2. Министерству цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан

1. Разработка общих стандартов и методических рекомендаций для обработки персональных данных с учетом потребностей общественных организаций.

2. Организация и проведение круглых столов с участием представителей общественных организаций, государственных органов в области защиты персональных данных.

3. Разработка специализированных программ для оказания правовой и консультационной помощи общественным организациям по вопросам защиты персональных данных.

4. Организация и проведение обучающих семинаров, тренингов для представителей общественных организаций по разъяснению правовых норм защиты персональных данных.

5. Разработка и принятие Правил по уведомлению субъектов персональных данных о действиях с его персональными данными.

6. Разработка и принятие Правил по уничтожению персональных данных по истечении цели использования. Отсутствие четкой процедуры может внести неясности при самостоятельном осуществлении данной процедуры.

7. Разработка и принятие Перечня критериев, которые должны отвечать при согласии на сбор и обработку персональных данных (например, добровольность, отсутствие принуждения, информированность и т.д.). В действующем Законе отсутствует перечень критериев.

7. Ввести в понятийный аппарат термин «общедоступный источник», так как в Законе данное словосочетание используется в статье 7.

Комментарии к п.7

Отсутствие четкого понятия что такое общедоступный источник может нарушить права субъекта персональных данных.

Например, общедоступный источник может содержать информацию, которую субъект персональных данных не намеревался раскрывать. Также объединение персональных данных из различных общедоступных источников может привести к неверному представлению о человеке, что может негативно сказаться на его репутации или других аспектах жизни и другие потенциальные ситуации. Или использование неточных или устаревших персональных данных, опубликованных ранее в общедоступных источниках, может привести к неправильным выводам о человеке, что также может являться нарушением прав субъекта.

Имеется ответ Комитета по информационной безопасности Министерства на заданный вопрос заявителя: «Допустимо ли любую онлайн—платформу или иной источник, содержащий общедоступную информацию, т.е. информацию, которая не может быть ограничена в силу требований законов либо которую раскрывает (распространяет) само лицо (физическое или юридическое) относить общедоступной?» Комитет отвечает, что **«...социальные сети допустимо относить к общедоступным источникам.»**

Однако, согласно ст.60 Закона «О правовых актах» **Такие разъяснения не имеют обязательной юридической силы и носят рекомендательный характер.**

8. Уточнить условия при повторном сборе, обработке и распространении третьими лицами персональных данных, так как в действующем Законе отсутствует требование о согласии при повторном сборе. (пункты 3,4 ст.7 Закона).

ЗАКЛЮЧЕНИЕ

Особенно актуальными сейчас являются аспекты защиты, сбора, обработки и хранения персональных данных организациями при приеме на работу работников, тонкости обмена персональными данными во время заключения договоров, защита личных данных в сети Интернет, а также вопросы хранения и уничтожения персональных данных.

Кроме того, общественные организации, работающие в различных сферах, от здравоохранения до образования и социальной помощи, обладают особыми обязательствами по обеспечению конфиденциальности и безопасности данных своих участников, волонтёров и клиентов.

Выработав эффективную стратегию управления в области защиты персональных данных от мошенничества, неправомерного использования данных можно добиться баланса между использованием технологий для оптимизации работы и защитой прав граждан на конфиденциальность и безопасность своих данных.

Правильное и грамотное управление защиты персональных данных позволит предотвратить утечку данных, укрепить доверие со стороны заинтересованных лиц, что является ключевым аспектом устойчивого развития любой организации.

Общественные организации должны активно рассматривать риски и вызовы, связанные с защитой персональных данных, и разрабатывать стратегические подходы для их минимизации.

На сегодняшний день существует множество инструментов и методов для обеспечения безопасности персональных данных, среди которых можно выделить шифрование, использование системы контроля доступа, регулярные аудиты и обучение сотрудников.

Важно отметить, что человеческий фактор часто играет решающую роль в вопросах безопасности, поэтому обучение и повышение осведомленности сотрудников о рисках и методах защиты должны стать приоритетом для каждой общественной организации.

Особо хотелось обратить внимание на ключевые действия для достижения цели по обеспечению безопасности персональных данных в организациях:

1. Политика безопасности.
2. Оценка рисков.
3. Обучение работников.
4. Технические меры защиты.
5. Мониторинг и реагирование.

Также следует учитывать необходимость соблюдения не только национального законодательства но и стандартов в области защиты данных, таких как GDPR. Это не только поможет избежать правовых последствий, но и станет залогом хорошей репутации и конкурентоспособности организации.

Общественным организациям необходимо проявлять инициативу по совершенствованию законодательства по защите персональных данных. Эти инициативы в дальнейшем сформируют безопасную среду для обработки личной информации.

Таким образом, комплексное внедрение мер по повышению безопасности персональных данных в общественных организациях является не просто необходимостью, но и стратегическим выбором на стабильность в условиях быстро меняющейся цифровой среды.

Защита персональных данных в общественных организациях – это не просто юридическая обязанность, но и важный аспект их социальной ответственности.

Необходимо отметить, что повышение осведомленности населения о защите персональных данных, о цифровых правах позволит создать устойчивую экосистему в обществе.

Успешная реализация мер по защите данных будет способствовать не только соблюдению законодательства, но и становлению общественных организаций как надежных и открытых институтов, способствующих развитию гражданского общества.

СПИСОК ЛИТЕРАТУРЫ

1. Всеобщая декларация прав человека, Принята резолюцией 217A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года.

2. Международный пакт о гражданских и политических правах, Принят резолюцией 2200 A (XX1) Генеральной Ассамблеи от 16 декабря 1966 года.

3. «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» принятый членами Совета Европы 28 января 1981 году.

4. Конституция Республики Казахстан, принята на республиканском референдуме 30 августа 1995 года.

5. Закон Республики Казахстан «О персональных данных и их защите» принят 21 мая 2013 года № 94-V.

6. https://kapital.kz/tehnology/128514/v-rk-rastet-chislo-pravonarusheniy-svyazannykh-s-zashchitoy-personal-nykh-dannykh.html.

7. https://liter.kz/v-kazakhstane-proveli-proverki-na-12-mln-tenge-v-sfere-zashchity-personalnykh-dannykh-1742455826/

8. https://www.gov.kz/memleket/entities/inf/activities/142?lang=ru

ИНМИР

ERKINDIK QANATY
общественный фонд

INSTITUTE FOR WAR & PEACE REPORTING
IWPR
ИНСТИТУТ РЕПОРТАЖЕЙ ВОЙНЫ И МИРА