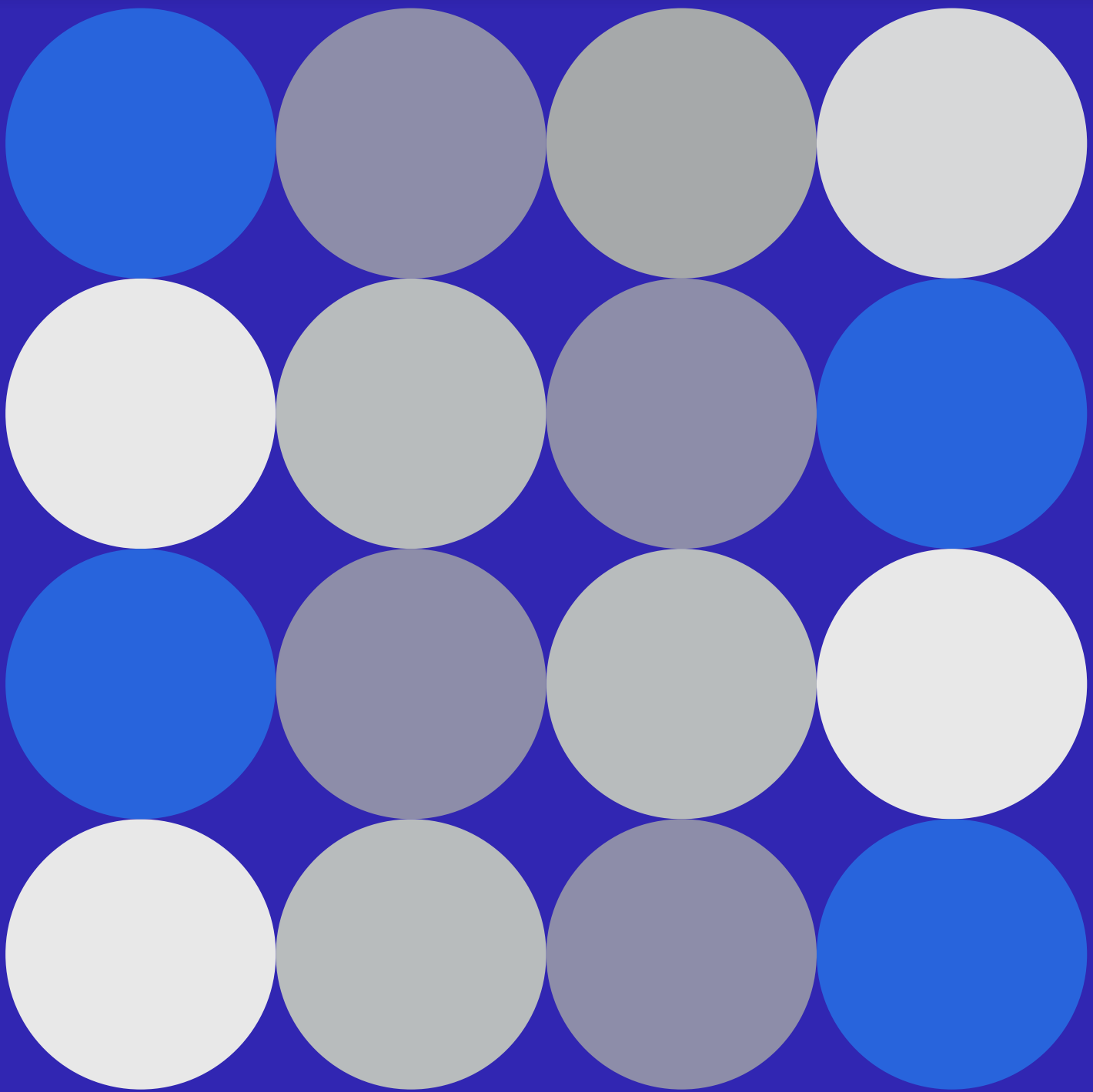
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ И ДРУГИЕ ИЗМЕНЕНИЯ.

GRATA INTERNATIONAL



ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ И ДРУГИЕ ИЗМЕНЕНИЯ.

11 февраля 2024 года был введен в действие Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» (далее – «Закон») от 11 декабря 2023 года № 44-VIII ЗРК. Законом предусматривается ряд существенных изменений и дополнений в Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года N 94-V (далее – «Закон о Персональных Данных»).

Отметим ключевые изменения:

1. Введено понятие «нарушение безопасности персональных данных».
2. С 1 июля 2024 года вводится обязанность уведомлять Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (МЦРИАП) о нарушении безопасности персональных данных.
3. Введен запрет на сбор и обработку бумажных копий документов, удостоверяющих личность.
4. Введен государственный контроль за соблюдением законодательства о персональных данных и их защите с наделением МЦРИАП соответствующими полномочиями.

Внесенные в Закон о Персональных Данных изменения требуют от субъектов предпринимательства более ответственного подхода к сбору и обработке персональных данных. Закон наделил МЦРИАП соответствующими полномочиями проводить внеплановую проверку субъектов предпринимательства на предмет соблюдения требований Закона о Персональных Данных. Для проверки требуется наличие конкретного факта и обстоятельства в отношении конкретного субъекта предпринимательства, к примеру обращение физического лица. О назначении внеплановой проверки МЦРИАП выносит акт, который обязательно регистрируется в Комитете по правовой статистике и специальным учетам Генеральной прокуратуры РК. В процессе проверки МЦИРАП проверяет исполнение субъектом предпринимательства требований, содержащихся в проверочном листе. В отношении законодательства о персональных данных проверочный лист содержит 33 требования. Однако, для некоторых субъектов предпринимательства не все требования являются обязательными. По результатам государственного контроля (проверки) МЦРИАП вынесет акт и предписание об устранении выявленных нарушений согласно проверочному листу. При этом, отдельно от государственного контроля, субъект предпринимательства может быть привлечен к административной ответственности, если будут основания для

возбуждения дела об административном правонарушении.

В приложении приводится обзор последних изменений и дополнений в Закон о Персональных Данных.

Как минимизировать риски ответственности и обеспечить соблюдение законодательства о персональных данных?

Чтобы минимизировать риски возможного нарушения законодательства о защите персональных данных и ответственности, компаниям необходимо:

1. Определить цели обработки персональных данных ограниченного доступа.
2. Определить порядок обработки, распространения и доступа к персональным данным ограниченного доступа.
3. Определить порядок блокирования персональных данных ограниченного доступа при обращении субъекта данных.
4. Утвердить перечень персональных данных, необходимых и достаточных для выполнения осуществляемых задач.
5. Иметь базу на территории РК, в которой хранятся персональные данные ограниченного доступа.
6. Утвердить политику сбора, обработки и защиты персональных данных.
7. Выделить бизнес-процессы, содержащие персональные данные ограниченного доступа.
8. Разделить персональные данные на общедоступные и ограниченного доступа.
9. Определить перечень лиц, осуществляющих сбор и обработку персональных данных либо имеющих к ним доступ.
10. Назначить лицо, ответственное за организацию обработки персональных данных (для юридических лиц).
11. Обеспечить установку средств защиты информации, обновлений программного обеспечения на технических средствах, осуществляющих обработку персональных данных ограниченного доступа.
12. Внедрить ведение (1) журнала событий систем управления базами при обработке персональных данных ограниченного доступа и (2) журнала действий пользователей, имеющих доступ к персональным данным ограниченного доступа.
13. Внедрить применение средств контроля целостности персональных данных ограниченного доступа.
14. Внедрить использование криптографических средств защиты информации и шифрования при хранении и передаче персональных данных.
15. Внедрить применение средств идентификации и (или) аутентификации пользователей при работе с персональными данными ограниченного доступа.

16. Иметь возможность подтвердить обеспечение защиты персональных данных в государствах, в которые осуществляется трансграничная передача персональных данных.

Выполнение указанных обязательств является комплексной задачей, которую следует выполнять отделу информационных технологий компаний совместно с юристами с целью минимизации негативных последствий и рисков.

Этот обзор предоставлен только в информационных целях. Хотя он предлагает общее понимание, он не является юридической консультацией. Для получения подробной помощи, адаптированной к вашей конкретной ситуации, мы рекомендуем вам связаться с юридической фирмой GRATA по адресу almaty@gratanet.com.

С уважением,

Юридическая фирма «GRATA»

1. НАРУШЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Закон ввел новое понятие «нарушение безопасности персональных данных»[1], которым признается «нарушение защиты персональных данных, повлекшее незаконное распространение, изменение и уничтожение, несанкционированное распространение передаваемых, хранимых или иным образом обрабатываемых персональных данных или несанкционированный доступ к ним».

Разработчики Закона объяснили введение данного понятия необходимостью определить утечку персональных данных, которая может нанести серьезный вред правам и интересам физических лиц.

Исходя из нового понятия в Законе о Персональных Данных, безопасность данных — это состояние их защищенности от незаконного и несанкционированного доступа и обработки, включая изменение, уничтожение, передачу, распространение, хранение персональных данных. Такое состояние защищенности обеспечивается соблюдением обязанностей собственника[2], оператора[3], согласно статьям 22 и 25 Закона о Персональных Данных. В частности, безопасность персональных данных обеспечивается организационными, техническими, правовыми мерами, которые обязан предпринимать и соблюдать собственник, оператор и третье лицо[4]. К числу указанных мер относится наличие правил, процедур и внутренних политик по сбору, обработке, хранению, передаче данных, регулированию доступа к персональным данным, установление средств защиты и прочие меры.

2. УВЕДОМЛЕНИЕ О НАРУШЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

С 1 июля 2024 года введена новая обязанность для собственника и оператора уведомить уполномоченный орган (МЦРИАП) о нарушении безопасности персональных данных в

[1] Подпункт 1) пункта 11 статьи 1 Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» от 11 декабря 2023 года № 44-VIII ЗРК

[2] Собственник базы, содержащей персональные данные – это государственный орган, физическое и (или) юридическое лицо, реализующие в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные данные.

[3] Оператор базы, содержащей персональные данные – это государственный орган, физическое и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных.

[4] 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.

течение одного рабочего дня с момента обнаружения нарушения[5]. В уведомлении должны быть указаны контактные данные лица, ответственного за организацию обработки персональных данных (при наличии). Далее, уполномоченный орган направляет оператору информационно-коммуникационной инфраструктуры «электронного правительства» (Акционерное общество «Национальные информационные технологии») информацию о нарушении безопасности персональных данных, если такое нарушение безопасности данных влечет риск нарушения прав и законных интересов субъектов персональных данных. Таким образом, новая норма внедряет механизм предупреждения уполномоченного органа и оператора «электронного правительства» о нарушениях безопасности персональных данных, влекущих риск нарушения прав и законных интересов субъектов персональных данных. Новая норма устанавливает строго определенный порядок действий собственников и операторов в случае обнаружения нарушений безопасности персональных данных. Это позволит более оперативно реагировать на нарушения и минимизировать возможные последствия для субъектов персональных данных. Кроме того, соответствующие поправки также внесены в Закон РК «Об информатизации» от 24 ноября 2015 года.[6]

Важно отметить, что обязанность уведомлять о нарушении безопасности данных вводится в действие только с 1 июля 2024 года. Но бизнесу следует минимизировать возможные риски и ответственность и реализовать до 1 июля 2024 года обязанности, предусмотренные Законом о Персональных Данных. Многие организации еще не разработали и не приняли требуемые законодательством документы, процедуры и политики по защите персональных данных, не назначили лицо, ответственное за организацию обработки персональных данных, не предприняли иные меры по защите персональных данных. Ниже мы укажем, на что следует обращать внимание бизнесу.

3. ЗАПРЕТ НА СБОР И ОБРАБОТКУ БУМАЖНЫХ КОПИЙ ДОКУМЕНТОВ, УДОСТОВЕРЯЮЩИХ ЛИЧНОСТЬ.

Законом введен запрет на сбор и обработку бумажных копий документов,

[5] Подпункт 4) пункта 11 статьи 1 Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» от 11 декабря 2023 года № 44-VIII ЗРК. См. также подпункт 8 пункта 2 статьи 25 Закона о Персональных Данных («Права и обязанности собственника и (или) оператора, лица, ответственного за организацию обработки персональных данных»)

[6] Пункт 12 статьи 1 Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» от 11 декабря 2023 года № 44-VIII ЗРК

удостоверяющих личность[7]. Запрет в том числе касается документов, удостоверяющих личность, сформированных сервисом цифровых документов «электронного правительства», так как они равнозначны документам на бумажном носителе.

Законом также установлены случаи, на которые данный запрет не распространяется. Собирать и обрабатывать бумажные копии удостоверяющих личность документов разрешено если:

- у собственника, оператора, третьего лица нет интеграции с объектами информатизации государственных органов и (или) государственных юридических лиц;
- у собственника, оператора, третьего лица нет возможности идентифицировать субъекта персональных данных с использованием технологических средств;
- в иных случаях, предусмотренных законами Республики Казахстан.

По мнению разработчиков Закона, новые нормы о запрете сбора бумажных копий документов обеспечат защиту персональных данных и устранят причины и условия их утечки. Однако указанный выше перечень исключений из этого требования (запрета) вызывает вопросы интерпретации и правоприменения. Иными словами, любой собственник, оператор, третье лицо, не имеющее интеграции с электронным правительством или технологические средства идентификации, сохраняет право запрашивать у физического лица бумажные копии документов, удостоверяющих личность. Такой возможностью могут пользоваться, к примеру, частная компания-работодатель, арендодатель помещения, учреждение образования (школа, колледж, университет, курсы по обучению языка и т.д.), фитнес-центры и прочие организации. При таком подходе кажется сомнительным, смогут ли новые нормы о запрете сбора бумажных копий устранить причины утечки персональных данных.

Отдельно следует отметить, что запрет не распространяется на копии документов нерезидентов и трудовых мигрантов.

4. СБОР И ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ СОГЛАСИЯ СУБЪЕКТА

Дополнен перечень случаев, когда не требуется согласие субъекта данных на сбор и обработку персональных данных. Законом единому накопительному пенсионному фонду

[7] Подпункт 2) пункта 11 статьи 1 Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» от 11 декабря 2023 года № 44-VIII ЗРК

предоставлено право не получать согласие субъекта при открытии пенсионного счета, информировании о пенсионных накоплениях и условных пенсионных счетах[8]. Указанная новая норма способствует эффективности деятельности единого накопительного пенсионного фонда, позволяет сократить административные процедуры и упростить взаимодействие с участниками пенсионной системы.

5. ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ КАЗАХСТАН О ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ЗАЩИТЕ.

Закон наделил уполномоченный орган в сфере защиты персональных данных (далее – «Уполномоченный орган») дополнительными полномочиями[9]. Основным нововведением является государственный контроль за соблюдением законодательства Республики Казахстан о персональных данных и их защите[10], который будет осуществлять Уполномоченный орган - МЦРИАП.

При этом, новая статья 27-2 Закона о Персональных Данных устанавливает, что контролю подлежат не только субъекты предпринимательства, но и государственные органы. Если Предпринимательский Кодекс РК регламентирует порядок проведения государственного контроля в отношении субъектов предпринимательства, то статья 27-3 Закона о Персональных Данных отдельно устанавливает порядок проведения контроля за соблюдением законодательства о защите персональных данных в отношении государственных органов, Национального банка Республики Казахстан и его организаций.

5.1. ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ В ОТНОШЕНИИ ГОСУДАРСТВЕННЫХ ОРГАНОВ.

Закон о персональных данных дополнен статьей 27-3, устанавливающей порядок проведения государственного контроля в отношении государственных органов в форме

[8] Подпункт 3) пункта 11 Статьи 1 Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» от 11 декабря 2023 года № 44-VIII ЗРК
[9] Подпункт 5) пункта 11 Статьи 1 Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» от 11 декабря 2023 года № 44-VIII ЗРК
[10] Пункт 2 и подпункт 6) пункта 11 Статьи 1 Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» от 11 декабря 2023 года № 44-VIII ЗРК.

периодических и внеплановых проверок. Периодические проверки проводятся не чаще одного раза в год в соответствии с планом проведения периодических проверок, утвержденным первым руководителем Уполномоченного органа. Внеплановые проверки назначаются Уполномоченным органом и проводятся при наличии обращений физических и юридических лиц, требований прокуроров, обращений государственных органов и в других случаях.

Кроме того, статьей 27-3 Закона о персональных данных определены права и обязанности субъектов Государственного контроля, сроки проведения проверок, а также другие положения.

5.2. ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ В ОТНОШЕНИИ СУБЪЕКТОВ ПРЕДПРИНИМАТЕЛЬСТВА.

В соответствии с частью первой статьи 27-2 Закона о Персональных Данных, государственный контроль в отношении собственников и операторов, являющихся субъектами предпринимательства, будет осуществляться в форме внеплановой проверки в соответствии с Предпринимательским кодексом РК. Важно отметить, что для внеплановой проверки нужно основание - наличие конкретного факта и обстоятельства в отношении конкретного субъекта (объекта) контроля и надзора. Целью внеплановой проверки является предупреждение и (или) устранение непосредственной угрозы законным интересам физических лиц. Контролирующий орган (МЦРИАП) выносит акт о назначении внеплановой проверки,[11] который обязательно регистрируется в Комитете по правовой статистике и специальным учетам Генеральной прокуратуры РК.[12]

Предметом внеплановой проверки могут быть только те требования, которые содержатся в проверочных листах[13]. Стоит отметить, что в соответствии с требованиями подпункта 2) пункта 2 статьи 85 и статьи 143 Предпринимательского Кодекса РК принят Совместный приказ уполномоченных органов об утверждении проверочного листа за соблюдением законодательства о персональных данных[14]. Проверочный лист содержит 33 пункта обязательных требований, предъявляемых к

[11] Пункт 1 статьи 145 Предпринимательского Кодекса РК
[12] Пункт 1 статьи 146 Предпринимательского Кодекса РК
[13] Пункт 6 статьи 137 Предпринимательского кодекса РК.
[14] Совместный приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 19 марта 2024 года No 149/НҚ и приказ Заместителя Премьер-Министра - Министра национальной экономики Республики Казахстан от 19 марта 2024 года No 12. «Об утверждении проверочного листа за соблюдением законодательства Республики Казахстан о персональных данных и их защите в отношении собственников и (или) операторов, а также третьих лиц». Зарегистрирован в Министерстве юстиции Республики Казахстан 29 марта 2024 года No 34179.

деятельности собственников, операторов и третьих лиц. Отметим, что не все требования проверочного листа могут быть применимы к отдельным собственникам, операторам и третьим лицам. По результатам проведенной проверки проверяющий орган вынесет акт, в котором будут указаны пункты требований проверочного листа с выявленными нарушениями и предписание об их устранении.[15]

Следует отметить, что в ходе внеплановой проверки могут быть выявлены основания для возбуждения дела об административном правонарушении и наложения соответствующего административного взыскания.

[15] Статья 152 Предпринимательского Кодекса РК