ВМЕШАТЕЛЬСТВО В СЛУЧАЕ УТЕЧКИ ДАННЫХ

ПРАВИЛА ПЛАНИРОВАНИЯ

KVKK_Y2 ВЕРСИЯ 1.00

1. ЦЕЛЬ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Компания Kardelen Paint and Chemical Industry Trade Limited (далее именуемая «Компания»)

Настоящий План реагирования на утечку персональных данных (далее именуемый таковым) был принят нашей компанией в рамках стратегического планирования для обеспечения готовности компании к незамедлительным действиям в случае нарушений безопасности данных в соответствии с положением Уведомления о Решении № 2019/10 Совета по защите персональных данных от 24.01.2019 о порядке и принципах уведомления об утечках персональных данных, в котором говорится, что «В случае утечки данных контролер данных должен подготовить план реагирования на утечку данных, который включает такие вопросы, как кому сообщать в своей организации, кто несет ответственность в своей организации за уведомления, которые должны быть сделаны в рамках Закона, и оценку возможных последствий утечки данных, и что этот план должен пересматриваться через определенные интервалы». Основное внимание в плане реагирования, который будет реализован в случае любой утечки, будет уделено оперативным действиям по защите физических лиц и их персональных данных. Наша компания в первую очередь стремится выполнить следующие действия в случае утечки данных:

(a) Уведомить Совет по защите персональных данных (Совет) о нарушении защиты персональных данных без неоправданной задержки и не позднее чем через 72 часа после того, как станет известно о нарушении безопасности данных (Компания имеет право по своему усмотрению решать, уведомлять ли Совет, если нарушение защиты персональных данных вряд ли представляет угрозу для естественных прав и свобод).

(b) Уведомлять затронутых субъектов данных без неоправданной задержки, за исключением случаев, когда вероятность утечки персональных данных, приводящей к высокому риску для прав и свобод физических лиц, низка.

1.2. Настоящее Положение:

(a) Данное уведомление будет разослано всем соответствующим сторонам, занимающимся обработкой данных. Лица, выступающие в качестве обработчиков данных, обязаны незамедлительно уведомить нас, как только им станет известно о любом нарушении безопасности персональных данных, которые они обрабатывают от имени нашей Компании.

(b) Положения Плана действий будут доведены до сведения наших сотрудников при их вступлении в должность и будут обсуждаться на периодических собраниях персонала и учебных занятиях, чтобы обеспечить информированность персонала о плане.

1.3. Шаги, которые необходимо выполнить в соответствии с блок-схемой, являющейся частью настоящего Регламента.

Краткое изложение было сделано.

1.4. Определения: Ниже приведены определения, применимые к положениям настоящего Регламента.

Они перечислены следующим образом:

1.4.1. Осведомленность о нарушении: Контролер данных считается «осведомленным о нарушении», если он обладает разумной степенью уверенности в том, что произошло нарушение безопасности, которое ставит под угрозу безопасность персональных данных.

1.4.2. Ущерб: персональные данные, которые были изменены, повреждены или устарели.

1.4.3. Уничтожение: Данные, которые больше недоступны или которые контролер данных утратил каким-либо образом.
недоступно в форме, которую он/она может использовать.

1.4.4. Потеря: Данные могут оставаться доступными, но контролер утратил контроль над ними.
Они утратили контроль над данными или доступ к ним, либо больше ими не владеют.

1.4.5. Нарушение защиты персональных данных — это нарушение безопасности, которое приводит к случайному или незаконному уничтожению, потере, изменению, несанкционированному разглашению или несанкционированному доступу к персональным данным, передаваемым, хранящимся или обрабатываемым;

1.4.6. «Временная потеря данных»: делает персональные данные непригодными для использования в течение определенного периода времени.
событие, которое стало причиной этого.

1.4.7. «Несанкционированная или незаконная обработка» означает раскрытие (или доступ) к персональным данным получателям, не уполномоченным получать (или получать доступ) к данным, или любую другую форму обработки, нарушающую положения Закона № 6698.

1.5. Нарушение безопасности данных может произойти по разным причинам, в том числе по следующим:

• Человеческая ошибка

• Утеря или кража документов или устройств, содержащих персональные данные

• Несанкционированное проникновение, кража, ограбление

• Внедрение неадекватных средств контроля доступа, позволяющих несанкционированное использование/доступ.

• Сбои в работе оборудования и неадекватное резервное копирование системы.

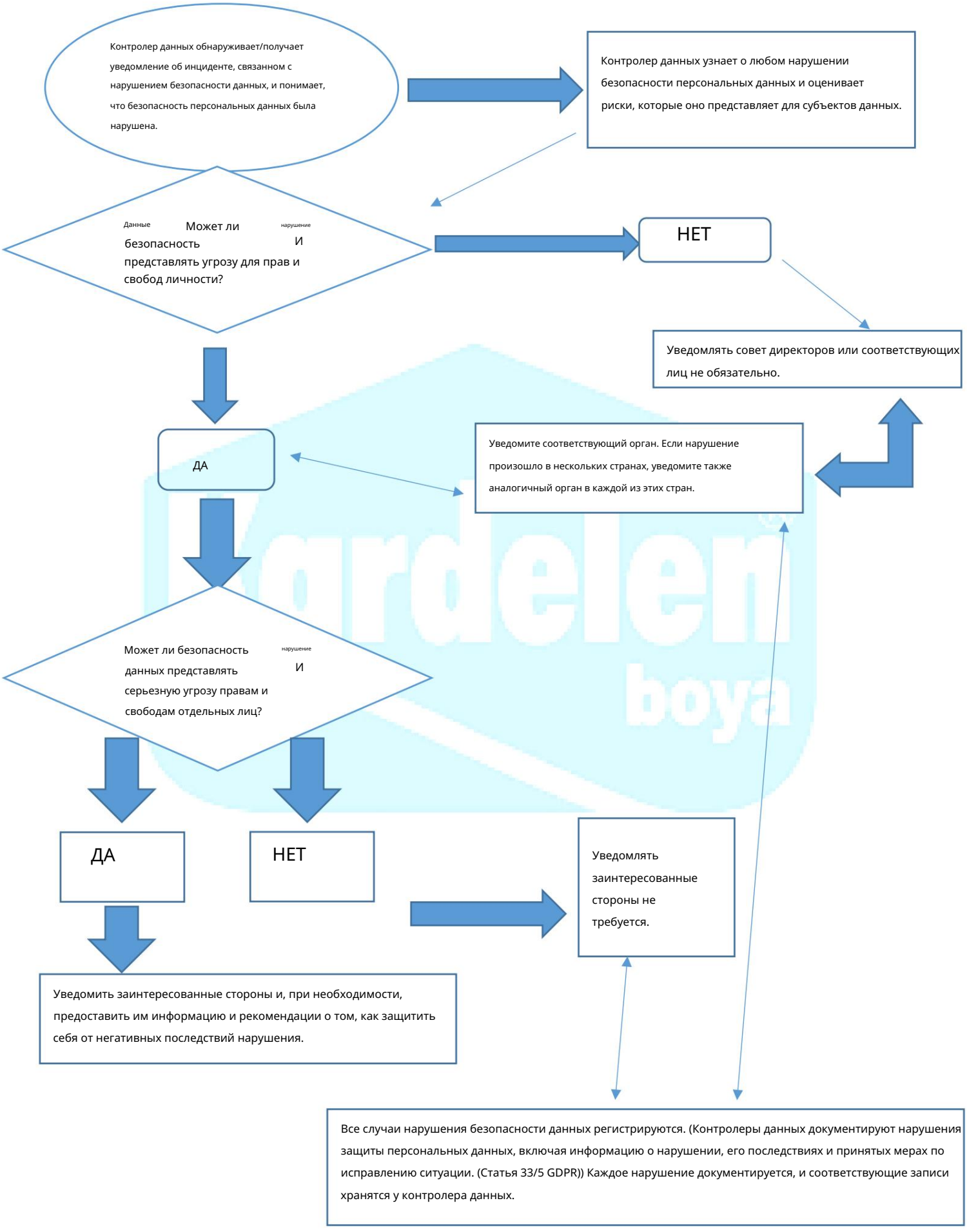
• Стихийные бедствия, такие как наводнения или пожары.

• Фишинг (незаконное получение пароля или данных кредитной карты путем отправки сообщений), электронное мошенничество или кража информации, когда личная информация получается обманным путем или мошенничеством.

• Злонамеренные кибератаки, такие как взлом, вредоносное ПО, атаки типа «отказ в обслуживании» (DoS-DDoS) или атаки программ-вымогателей.

1.6. Нарушения конфиденциальности персональных данных могут иметь негативные последствия для отдельных лиц, потенциально причиняя физический, материальный или моральный вред. Такие ситуации могут привести к смущению, стрессу или унижению для субъекта данных. Другие негативные последствия могут включать: потерю контроля над персональными данными, ограничение прав личности, дискриминацию, кражу личных данных или мошенничество, финансовые потери, ущерб репутации, потерю конфиденциальности персональных данных, защищенных профессиональной тайной, и значительные экономические или социальные недостатки для пострадавших лиц.

А. Блок-схема, описывающая обязанность сообщать о нарушениях.



1.7. Утечки персональных данных могут привести, например, к следующим ситуациям:

Это также может нанести вред нашей компании:

• Ущерб доверительным отношениям, которые мы выстроили с нашими сотрудниками и клиентами.

• Утеря, удаление или повреждение персональных данных, необходимых для управления нашей компанией.

видя,

• Ущерб корпоративной репутации нашей компании.

• Столкнуться с административными санкциями в соответствии с законодательством о защите данных или инициировать против нас

судебные иски и расследования с целью взыскания материального/морального ущерба.

2. ПЛАН ВМЕШАТЕЛЬСТВА

В случае возможного нарушения безопасности персональных данных Компания будет действовать в соответствии с планом реагирования, описанным ниже:

2.1. Выявление нарушения безопасности данных и информирование соответствующих должностных лиц о ситуации.

2.1.1. Сотрудник или менеджер по вопросам защиты данных[1] должен быть проинформирован как можно скорее.

будет сделано.

2.1.2. Сотрудник или руководитель, ответственный за защиту данных, обязан незамедлительно уведомить генерального директора.

Это предоставит информацию.

2.1.3. Сотрудник/менеджер по вопросам защиты данных сформирует небольшую группу, именуемую группой реагирования на кибер-инциденты (CIRT), для оценки потенциального ущерба, потерь, несанкционированного доступа, временной потери данных и принятия соответствующих мер по локализации нарушения/устранению ситуации и восстановлению состояния, предшествующего нарушению. Весь персонал, а также все обработчики данных и/или совместные контролеры данных обязаны оказывать всю необходимую помощь сотруднику/менеджеру по вопросам защиты данных и персоналу сформированной ими группы.

2.1.4. Сотрудник/менеджер по вопросам защиты данных должен подготовить письменную хронологию событий, в которой будут зафиксированы все аспекты нарушения, включая следующие:

(a) Дата и время сообщения о нарушении (в формате ДД/ММ/ГГГГ и 24-часовом формате времени).

(b) Если уведомление касается потенциального нарушения, необходимо указать подробности предварительного расследования (при необходимости), которое будет проведено для определения того, действительно ли произошло нарушение.

(c) Подробная информация о том, кто сообщил о случившемся.

(d) Что известно / что подозревается на этом начальном этапе.

(e) подробная информация о том, с какой системой/набором данных связана утечка данных.

(f) Оценка риска для прав и свобод физических лиц.

---

1. Сотрудник по связям с Советом директоров, ответственный за защиту данных, — это лицо, назначенное нашей компанией в качестве представителя в Совете директоров. Им может быть старший менеджер, назначенный в рамках административной структуры компании, специалист по защите данных, работающий в компании для этой цели, или юрист, привлеченный нами для этой цели.

(g) Действия, которые необходимо предпринять в срочном порядке (расследование, локализация ущерба, устранение последствий, восстановление данных и т. д.).

(h) Подробная информация о команде, собранной для оказания помощи.

(i) Подробное описание задач, назначенных каждому члену команды.

(j) Аналогично (g), в течение 72 часов с момента обнаружения нарушения, сообщить Совету. Необходимо уведомить.

(k) (при необходимости) уведомление пострадавших лиц без неоправданной задержки.

2.1.5. Независимо от того, было ли принято решение об уведомлении Совета, информация о каждом потенциальном, зарегистрированном или предполагаемом нарушении защиты персональных данных, включая его последствия и принятые меры по исправлению ситуации, должна быть задокументирована.

2.2. Ограничение нарушений безопасности, смягчение их последствий и
Меры по устранению

2.2.1. Компания незамедлительно предпримет шаги для локализации утечки и внедрит необходимые меры для предотвращения несанкционированного доступа к хранящимся персональным данным и ограничения любого связанного с этим ущерба.

2.2.2. В случае нарушения безопасности данных, затрагивающего информационные технологии (ИТ) и/или электронные данные, необходимо незамедлительно связаться с персоналом ИТ-поддержки компании для получения консультаций и технической помощи относительно необходимых мер, таких как ограничение ущерба, изоляция затронутых зон хранения данных и сохранение данных и журналов событий.

2.2.3. В зависимости от характера нарушения/угрозы защите персональных данных, принимаемые меры могут включать следующие шаги:

(а) Изолирование части или всех персональных компьютеров, сетей и т. д.

(б) Сотрудников следует предупредить о недопустимости доступа к компьютерам, сетям, устройствам и т. д.

(c) Приостановление действия учетных записей пользователей,

(d) Проверка записей, хранящихся на резервных серверах.

(e) Выявление типов персональных данных, которые могли быть потенциально раскрыты, и обстоятельств несанкционированного доступа.

2.2.4. При необходимости может быть рассмотрен вопрос о карантине зон регистрации данных, которые поддерживаются вручную или иными способами.

2.2.5. При необходимости может быть задействована группа по расследованию преступлений в сфере информационных технологий, а также может быть запрошена юридическая консультация.

2.3. Анализ рисков

2.3.1. В случае утечки персональных данных компания обязана провести всесторонний анализ рисков, чтобы определить, представляет ли утечка персональных данных угрозу правам и свободам физических лиц.

2.3.2. Категории риска, которые лягут в основу оценки, следующие:

- Отсутствие риска: Внедрение соответствующих технических и административных мер защиты, а также защита персональных данных с помощью таких мер, как шифрование, делающее данные нечитаемыми для лиц, не имеющих на них разрешения, наряду с дополнительными мерами предосторожности, гарантируют, что высокий риск для прав и свобод субъектов данных больше невозможен.
- Низкий риск: Участники могут преодолеть незначительные неудобства.
  Они могут столкнуться с (чрезмерными затратами времени, неудобствами и т. д.).
- Умеренный риск: у людей могут возникнуть трудности, которые они смогут преодолеть.
  (дополнительные усилия, дополнительные расходы, стресс, незначительный физический дискомфорт и т. д.)
- Высокий риск: Люди могут столкнуться с серьезными последствиями, которые им придется преодолеть (финансовый ущерб, потеря работы, судебное расследование, ухудшение здоровья и т. д.).
- Очень высокий риск: Люди могут столкнуться с непреодолимыми трудностями и необратимыми последствиями (прекращение работы, долгосрочные психологические и физические страдания, смерть и т. д.).

Если будет установлено, что никакой угрозы правам и свободам физических лиц не будет, причины, приведшие к такой оценке, будут зафиксированы.

2.3.3. При проведении анализа рисков Компания будет учитывать уровень конфиденциальности данных и категории вовлеченных лиц (например, дети, уязвимые лица), чтобы определить, подвергаются ли они большему риску в результате утечки данных.

2.3.4. Тот факт, что персональные данные надежно зашифрованы с использованием новейших методов шифрования и что ключи не были скомпрометированы в случае нарушения безопасности, может служить основанием для вывода о том, что утечка данных не представляет угрозы для прав и свобод отдельных лиц и что нет необходимости информировать Совет и владельцев данных.

2.3.5. При проведении анализа рисков компания будет учитывать рекомендации Совета директоров, Национального центра реагирования на кибер-инциденты (USOM) и Европейского агентства по сетевой и информационной безопасности (ENISA).

2.3.6. Если будет установлено, что информирование Совета и владельцев данных не является необходимым, причины такого решения будут задокументированы, и эта документация будет храниться в архиве для предъявления во время любых проверок, которые могут быть проведены Советом.

---

2 www.enisa.europa.eu/publications/dbn-severity

2.4. Уведомление соответствующих учреждений и лиц о нарушении

2.4.1. Сообщение о нарушениях безопасности данных в Совет по защите персональных данных: Все инциденты, в которых персональные данные и конфиденциальные персональные данные могут оказаться под угрозой (ситуации, не представляющие угрозы правам и свободам субъектов данных, не входят в эту сферу).
О происшествии будет сообщено Совету без неоправданной задержки и не позднее чем через 72 часа после получения уведомления о нарушении.

2.4.2. ЗАПОЛНЕНИЕ ФОРМЫ СООБЩЕНИЯ О НАРУШЕНИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ KVKK: После перехода на веб-сайт Управления по защите персональных данных по адресу www.kvkk.gov.tr, нажмите на значок «Сообщение о нарушении защиты персональных данных», расположенный в меню в правой части главной страницы, чтобы перейти в раздел сообщения о нарушении защиты персональных данных.

2.4.3. На странице входа размещено «ОБЪЯВЛЕНИЕ ОТНОСИТЕЛЬНО РЕШЕНИЯ СОВЕТА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ 24.01.2019 ЗА НОМЕРОМ 2019/10, КАСАЮЩЕГОСЯ ПРОЦЕДУР И ПРИНЦИПОВ УВЕДОМЛЕНИЯ О НАРУШЕНИЯХ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ». Вы можете перейти на страницу уведомления, нажав на форму уведомления о нарушении защиты персональных данных (Интернет), расположенную внизу этой страницы. Если вы хотите заполнить форму вручную, нажмите на форму уведомления о нарушении защиты персональных данных (PDF).

2.4.2. Уведомление в адрес Совета должно содержать как минимум следующие пункты:

- Информация об источнике нарушения и обстоятельствах его возникновения.
- Отдельные группы, пострадавшие от нарушения (например, дети, другие уязвимые группы, люди с инвалидностью,
  - Количество людей и записей,

пострадавших от утечки данных (по крайней мере, приблизительное).

- Категории персональных данных, затронутых утечкой (например, информация, удостоверяющая личность, данные об образовании, данные социального страхования, финансовая информация, номера банковских счетов, номера паспортов и данные о состоянии здоровья, а также особые категории данных, такие как раса и этническая принадлежность).
- Имя и контактная информация сотрудника/менеджера по вопросам защиты данных (контактная информация сотрудника, у которого можно получить подробную информацию)
- Описание потенциального воздействия утечки данных на пострадавших лиц (например, потеря контроля над персональными данными, кража личных данных, дискриминация, ограничение прав, мошенничество, финансовые потери, ущерб репутации, риск разглашения конфиденциальной профессиональной информации и т. д.).
- Описание административных и технических мер, принятых компанией до утечки данных, а также мер, принятых или запланированных для устранения последствий утечки. (Например, удаление ошибочно переданных данных, обеспечение безопасности паролей, планирование обучения по вопросам информационной безопасности и т. д.) По возможности, в этот раздел также будут включены меры, принятые для смягчения негативных последствий утечки данных.

- Важное примечание: Тот факт, что окончательная информация по перечисленным выше вопросам пока недоступна, не должен задерживать своевременное уведомление Совета. Следует отметить, что текущая информация будет передана, и учреждение будет немедленно проинформировано, как только появится более подробная информация.

2.4.3. В случаях, когда утечка данных подпадает под юрисдикцию судебных органов, правоохранительных органов или других государственных учреждений, расположенных за рубежом, и в отношении этой утечки...

Организации или учреждения, расположенные за рубежом, могут нуждаться в уведомлении. В случае уведомления документы, подтверждающие его отправку, должны быть зарегистрированы и представлены в Совет.
Его необходимо подать вместе с уведомлением.

2.4.4 Причины уведомления со стороны Компании:

(a) Избежание административных штрафов: статья 18 Закона № 6698 о защите персональных данных.
Неуведомление Совета в соответствии с соответствующей статьей может повлечь за собой административный штраф.

(b) Обращение за консультацией: Компания может обратиться за консультацией к Совету директоров относительно мер, которые необходимо предпринять в ответ на нарушение, и сотрудничество с Советом директоров важно для обоснования решений о том, информировать или не информировать владельцев затронутых данных.

2.4.5. Информирование соответствующих лиц, пострадавших от нарушения.

2.4.5.1. После проведения анализа рисков, упомянутого в разделе 2.3.1 выше, если утечка персональных данных, вероятно, представляет «высокий риск» для прав и свобод физических лиц, Компания обязана:

(a) С соответствующими сторонами свяжутся по телефону, электронной почте и т. д. без неоправданной задержки.

(b) Оно уведомит соответствующих лиц о произошедшей утечке данных.

(c) Оно предоставит субъектам данных подробную информацию по вопросам, описанным выше в пункте 2.4.2.

(d) В соответствующих случаях оно предоставит субъектам данных конкретные рекомендации о том, как защитить себя от потенциальных негативных последствий утечки данных (например, сброс пароля).

2.4.5.2. Уведомление субъекта данных должно четко и просто разъяснять характер нарушения защиты персональных данных и включать, как минимум, имя и контактную информацию сотрудника по защите данных или другого контактного лица, у которого можно получить дополнительную информацию, возможные последствия нарушения защиты персональных данных, а также, при необходимости, разъяснения мер, принятых или рекомендованных нашей компанией для устранения нарушения защиты персональных данных, включая меры по смягчению возможных негативных последствий нарушения защиты персональных данных.

2.4.6. Уведомление субъекта данных не является обязательным, если выполняется любое из следующих условий:

(a) Компания должна была внедрить соответствующие технические и административные меры защиты, включая такие меры, как шифрование, делающее персональные данные нечитаемыми для любого лица, не имеющего права доступа к ним, и эти меры должны были быть применены к персональным данным, затронутым утечкой;

(b) Компания должна принять дополнительные меры для обеспечения того, чтобы высокий риск для прав и свобод субъектов данных больше не представлялся возможным;

(c) Если уведомление потребует чрезмерных усилий. В этом случае вместо него следует применить публичное уведомление или аналогичную меру, в рамках которой субъекты данных будут проинформированы с той же эффективностью.

2.4.7. Уведомление правоохранительных органов

(a) В случае несанкционированного доступа к персональным данным, об этом следует незамедлительно сообщить в соответствующий правоохранительный орган.

(b) В зависимости от характера персональных данных, находящихся под угрозой, и особенно в случаях, когда под угрозой могут находиться конфиденциальные персональные данные, следует обратиться за дополнительной помощью в правоохранительные органы.

(c) В случае «повреждения» данных необходимо сообщить об этом в правоохранительные органы. Невыполнение этого требования может повлечь за собой для Компании штрафные санкции и меры безопасности.

2.4.8. Другие учреждения и организации: При необходимости можно уведомить Министерство здравоохранения, Министерство по делам семьи и социальной политики, финансовые учреждения и другие соответствующие министерства и организации.

2.4.9. Компания уведомит страховую компанию, с которой заключен страховой договор, и сообщит ей о нарушении безопасности персональных данных.

2.5. Использование юридических консультаций и услуг адвокатов: Компания может информировать заинтересованные стороны, от которых она получает юридические консультации и услуги адвокатов, а также уведомлять их о нарушении безопасности персональных данных с целью получения юридической консультации, защиты в потенциальных судебных процессах, урегулирования споров или достижения других мирных решений.

2.6. Действия, которые необходимо предпринять после нарушения: После принятия необходимых мер экстренного реагирования на начальном этапе, в разумные сроки следует провести полную оценку и анализ произошедшего нарушения. В ходе этого процесса будут учитываться следующие моменты:

2.6.1. Будет подтверждено, что случаи утечки персональных данных задокументированы, включая информацию об утечке персональных данных, ее последствиях и принятых мерах по исправлению ситуации.

2.6.2. Необходимо определить выводы, сделанные на основе инцидента, аспекты, требующие улучшения, и детали принимаемых мер.

2.6.3 Компания обязана запросить у своего сотрудника по связям с общественностью/прокурора по вопросам защиты данных (и/или других внешних экспертов, чей опыт может быть использован для оказания ей помощи) соответствующее справочное заключение и отчет о расследовании, а также сохранить копию переписки, которой обменивались с Советом директоров и/или соответствующими сторонами, пострадавшими от нарушения.

2.6.4 Компания тщательно рассмотрит вопрос о целесообразности инициирования дисциплинарных мер в случае необходимости.

2.6.5. В случаях, когда необходимы корректирующие действия, ответственность возлагается на соответствующих должностных лиц, которым поручается обеспечить выполнение необходимых действий в установленные сроки в соответствии с их сферой ответственности.

2.6.6 Персонал должен быть проинформирован о любых изменениях в настоящем Плане реагирования и об обновленных мерах безопасности. При необходимости персонал должен пройти повторное обучение.

ПРИЛОЖЕНИЕ - ПРИМЕР ОТЧЕТА О НАРУШЕНИИ

ОТЧЕТ О НАРУШЕНИИ БЕЗОПАСНОСТИ ДАННЫХ

ТОЛЬКО ДЛЯ ИСПОЛЬЗОВАНИЯ КРАСКИ KARDELEN.

Нарушение защиты персональных данных: это нарушение безопасности, которое приводит к случайному или незаконному уничтожению, потере, изменению, несанкционированному разглашению или несанкционированному доступу к персональным данным, которые передаются, хранятся или обрабатываются.

Номер для отслеживания нарушений:	
Когда произошло нарушение безопасности данных?	
Где произошло нарушение безопасности данных?	Место, где произошло нарушение
Когда было сообщено о нарушении?	Пожалуйста, укажите дату и время.
Кто сообщил о нарушении безопасности?	
Контактная информация лица, сообщившего об утечке данных?	
Было ли направлено уведомление в Совет по защите персональных данных?	Да Нет
Если ответ «Да», пожалуйста, укажите способ уведомления (телефон, электронная почта и т. д.), а также дату и время уведомления.	
Если ответ «Нет», то связывались ли с кем-либо из других высокопоставленных должностных лиц, директоров и т. д., и если да, то каким способом (например, по телефону, электронной почте и т. д.), а также указав время и дату контакта?	
Есть ли свидетели инцидента? Если ответ «Да», пожалуйста, укажите их имена и контактные телефоны.	

Пожалуйста, предоставьте информацию об источнике нарушения.
Предоставьте подробную информацию о том, как произошло нарушение.
Пожалуйста, предоставьте информацию о категориях заинтересованных сторон, затронутых или потенциально затронутых нарушением (стажеры, сотрудники, соискатели, клиенты, поставщики, подрядчики и т. д.).
Каково количество лиц и записей, затронутых или потенциально затронутых утечкой данных? (Если количество лиц и/или записей является приблизительным, пожалуйста, объясните, почему точное число определить невозможно.)
Какие категории персональных данных пострадали от утечки? (Идентификационные данные, контактная информация, местоположение, персональные данные, судебные разбирательства, операции с клиентами, физическая безопасность, безопасность транзакций, управление рисками, финансы, профессиональный опыт, маркетинг, аудио- и видеозаписи, раса и этническая принадлежность, политические взгляды, философские убеждения, одежда, членство в ассоциациях, информация о здоровье, судимости и меры безопасности, биометрические данные и т. д.)

Опишите потенциальные последствия утечки данных для пострадавших лиц. (Потеря контроля над персональными данными, кража личных данных, дискриминация, ограничение прав, мошенничество, финансовые потери, ущерб репутации, потеря безопасности персональных данных и т. д.)
Пожалуйста, опишите меры, принятые или предложенные Компанией для устранения утечки персональных данных, включая меры по смягчению потенциальных негативных последствий утечки персональных данных. Важное примечание: Неосведомленность о деталях вышеупомянутых мер не является основанием для отказа от уведомления Совета по защите персональных данных. Информация может предоставляться поэтапно без каких-либо неоправданных задержек. В этом случае, пожалуйста, четко укажите это.
Считаете ли вы, что нарушение безопасности данных — это временная ситуация? Возможно ли восстановить скомпрометированные персональные данные и получить к ним доступ?

Были ли затронуты какие-либо ИТ-системы в результате инцидента? (например, электронная почта, веб-сайт, облачные программы, системы электронного документооборота и т. д.) Если да, пожалуйста, перечислите их ниже.
Доступны ли какие-либо дополнительные информационные материалы, такие как сообщения об ошибках, скриншоты, файлы журналов или записи с камер видеонаблюдения?
Предпринимали ли вы какие-либо действия для устранения/смягчения рисков для субъектов данных, которые, по вашему мнению, могли пострадать, или для других субъектов данных, которые, по вашему мнению, могли пострадать? Если ваш ответ «ДА», пожалуйста, объясните ниже.
Сообщили ли вы об этом кому-либо из руководства компании, например, члену совета директоров, генеральному директору или руководителю ИТ-отдела? Если ответ «ДА», пожалуйста, кратко опишите, с кем вы разговаривали и какие советы или инструкции получили во время разговора.
Обращались ли вы к каким-либо сторонним организациям, например, к страховым компаниям, IT-провайдерам, правоохранительным органам и т. д.? Если ответ «ДА», пожалуйста, опишите ниже, к кому вы обращались, и укажите их имена и контактную информацию.

.

Если у вас есть какие-либо дополнительные вопросы, пожалуйста, укажите их ниже.

Редактор:	
Ваша задача:	
Офицер Существование Единица:	
Ваши контактные данные: (желательно, ваш номер телефона)	
История:	
Время завершения составления отчета:	

Благодарим вас за заполнение этой формы. Заполнение этой формы поможет Карделен Боя лучше расследовать/анализировать данное дело.
Просим направить этот отчет непосредственно сотруднику/профессору компании, ответственному за защиту данных:

Сотрудник/руководитель по вопросам защиты данных:

Имя и фамилия:
Должность:
Адрес:
Телефон:
Электронная почта:

*ДАННАЯ ФОРМА СОСТАВЛЕНА С УЧЕТОМ ГРАЖДАНСКИХ И УГОЛОВНЫХ ДЕЛ.

ДОВОЖУ ДО ВАШЕГО СВЕДЕНИЯ:

Нарушения безопасности данных классифицируются в соответствии со следующими общепринятыми принципами информационной безопасности:

A) Конфиденциальность данных: это означает предотвращение доступа к данным со стороны неавторизованных лиц. «Нарушение конфиденциальности» означает несанкционированное или случайное разглашение или доступ к персональным данным.

B) Целостность данных: Это означает обеспечение надлежащего хранения и защиты данных. «Нарушение целостности данных» означает несанкционированное или случайное изменение персональных данных.

C) Доступность данных: Это означает, что данные всегда доступны и пригодны для использования. «Нарушение доступа» означает случайную или несанкционированную потерю доступа к персональным данным, или случайное или несанкционированное уничтожение персональных данных.

В зависимости от обстоятельств, нарушение безопасности данных может произойти из-за нарушения конфиденциальности, целостности и доступности персональных данных, или из-за сочетания этих факторов. Информация, помогающая определить, произошло ли нарушение конфиденциальности или целостности, относительно очевидна. Однако определить, было ли нарушено право на доступность данных, может быть сложнее. Если персональные данные безвозвратно утеряны или уничтожены, это всегда будет считаться нарушением принципа доступности данных.

ПРОЦЕДУРЫ, КОТОРЫЕ НЕОБХОДИМО СОБЛЮДАТЬ ПРИ РЕАГИРОВАНИИ НА НАРУШЕНИЯ БЕЗОПАСНОСТИ.

Чего делать не следует:

ЧЕМ ЗАНЯТЬСЯ:

- Увеличение числа случаев несанкционированного доступа, утечки данных, повреждения систем учета и т. д.

  Для предотвращения дальнейших инцидентов необходимо немедленно изолировать затронутую систему.

- Используйте телефон для связи. Злоумышленники могут отслеживать переписку по электронной почте.
- Немедленно свяжитесь с сотрудником/менеджером компании, ответственным за защиту данных.

  Специалист/менеджер по вопросам защиты данных:

  Имя и фамилия:

  Должность:

  Адрес:

  Телефон:

  Электронная почта:

- Сохраняйте все соответствующие записи журналов, например, межсетевого экрана, маршрутизатора и системы обнаружения вторжений.
- Создавайте резервные копии поврежденных или измененных файлов и сохраняйте эти резервные копии. Храните его в безопасном месте.
- Определите местоположение затронутой системы в топологии сети.
- Определите все системы и устройства, подключенные к затронутой системе.
- Программы и процессы, работающие в затронутой системе (системах), последствия сбоя и права доступа.

  Укажите максимально допустимую продолжительность отключения электроэнергии.

- Если будут собраны доказательства неисправности системы, примите меры для обеспечения непрерывности обслуживания, т.е. подготовьте резервную систему и создайте резервные копии данных.

Чего делать не следует:

• Не удаляйте, не перемещайте и не изменяйте файлы в затронутых системах. • Не связывайтесь с предполагаемыми злоумышленниками. • Не проводите анализ цифровых преступлений без соответствующего разрешения.

ДАННАЯ ФОРМА ДОЛЖНА БЫТЬ ЗАПОЛНЕНА ТОЛЬКО ГРУППОЙ ПО РЕАГИРОВАНИЮ НА УТЕЧКУ ДАННЫХ SOME-DATA.

Специалист/менеджер по вопросам защиты данных:	
Дата и время подачи данной формы в компанию:	
Пожалуйста, укажите последствия нарушения безопасности данных. Конфиденциальность данных, целостность данных, доступ к данным (см. пояснения выше)	
Количество лиц и записей, пострадавших от утечки данных	Примерное количество лиц и записей, пострадавших от утечки данных? Какие категории данных затронуты?
В результате утечки данных, какие особые категории персональных данных (расовая и этническая принадлежность, политические взгляды, религиозные и философские убеждения, принадлежность к определенной конфессии и другим убеждениям, членство в ассоциациях и профсоюзах, биометрические и генетические данные, информация о здоровье, особые категории персональных данных сексуального характера) были затронуты? Пожалуйста, укажите соответствующую информацию ниже. Например, скольким категориям персональных данных субъектов данных была нанесена утечка? (Жизнь) пострадала.	Да Нет
Существует вероятность того, что соответствующие лица могут подвергнуться неблагоприятным последствиям. Случайное или незаконное уничтожение, потеря, изменение, несанкционированное разглашение или несанкционированный доступ к передаваемым, хранящимся или обрабатываемым персональным данным представляют собой нарушение безопасности. Масштаб утечки данных следует определять, оценивая ее потенциальное воздействие на пострадавших лиц. При такой оценке необходимо учитывать характер и причину утечки, тип задействованных данных, меры, принятые для смягчения ее последствий, а также категории пострадавших лиц. * Если оценка риска не проводилась, пожалуйста, объясните причины:	 Очень высокий уровень риска: отдельные лица могут столкнуться с непреодолимыми трудностями и необратимыми последствиями (прекращение работы, долгосрочные психологические и физические страдания, смерть и т. д.).  Высокий уровень риска: Участники инцидента могут столкнуться с серьезными последствиями, которые им придется преодолеть (материальный ущерб, потеря работы, судебное расследование, ухудшение здоровья и т. д.).  Умеренная сложность: Люди могут столкнуться с управляемыми трудностями (чрезмерные усилия, дополнительные расходы, стресс, незначительный физический дискомфорт и т. д.).  Низкий уровень: Люди могут столкнуться с незначительными трудностями, которые они способны преодолеть (например, слишком много времени, скука).  Отсутствие риска: Внедрение соответствующих технических и административных мер защиты, а также защита персональных данных с помощью таких мер, как шифрование, делающее их нечитаемыми для любого лица, не имеющего разрешения на доступ к ним, гарантируют, что высокий риск для прав и свобод субъектов данных больше не существует.

Были ли проинформированы руководители высшего звена, входящие в совет директоров?	Да Нет
Уведомлен ли поставщик ИТ-услуг/группа технической поддержки?	Да Нет
Была ли страховая компания уведомлена?	Да Нет
Было ли подано заявление/жалоба в правоохранительные органы?	Да Нет
Были ли юридические консультанты проинформированы?	Да Нет
Были ли уведомлены соответствующие лица? Количество вовлеченных лиц? Существуют ли какие-либо списки контактов, которые позволили бы нам связаться с нужными людьми? Или есть ли возможность восстановить контактную информацию?	Да Нет
Было ли направлено уведомление в Совет по защите персональных данных? Управление по защите персональных данных Телефон: 0312 216 50 00 Колл-центр: ALO 198 Горячая линия по защите данных Информационно-консультационный центр Электронная почта: veriguvenligi@kvkk.gov.tr Веб-страница с формой уведомления о нарушении: https://www.kvkk.gov.tr/Icerik/5362/Veri-Breach-Notification Адрес: район Насух Акар, улица 1407. № 4, 06520 Чанкая/Анкара	Да Нет Если ответ «ДА», пожалуйста, укажите дату и время уведомления (если применимо). Ниже запишите полученные от учреждения рекомендации и инструкции:
Другие важные моменты	
Подпись сотрудника/менеджера, ответственного за защиту данных:	
Генеральный директор или назначенный им человек Подпись представителя:	
История:	

*Эта форма предназначена для использования в гражданских и уголовных делах.
ПОДГОТОВЛЕНО, ЕСЛИ ЭТО БЫЛО ДОСТУПНО.