ПЕРЕДАЧА ДАННЫХ

ПРОЦЕДУРЫ БЕЗОПАСНОСТИ И

О ЕГО ПРИНЦИПАХ ПРАВИЛА

KVKK_Y8 ВЕРСИЯ 1.00

Компания KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED

ПРОЦЕДУРЫ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ ПРАВИЛА, КАСАЮЩИЕСЯ

1. ЦЕЛЬ И ОБЛАСТЬ ПРИМЕНЕНИЯ

В ходе своей экономической деятельности наша компания хранит большой объем данных, как в электронном, так и в бумажном виде. Настоящее Положение о процедурах и принципах обеспечения безопасности передачи данных (далее именуемое «Положение») направлено на регулирование процедур, применимых к защите хранимых данных, и обеспечение безопасной передачи персональных данных внутри и за пределы компании.

Настоящее Положение распространяется на все следующие группы лиц в нашей Компании, которые обрабатывают персональные данные и конфиденциальные персональные данные и обязаны передавать эти данные заинтересованным сторонам Компании в рамках своих должностных обязанностей:

• Сотрудники •
Поставщики и подрядчики, с которыми сотрудничает наша компания • Стажеры

Наши сотрудники должны ознакомиться с данным Положением в совокупности с Положением о порядке и принципах использования информационно-коммуникационных технологий и Политикой информационной безопасности. Им следует это купить.

2. СООТВЕТСТВУЮЩЕЕ ЗАКОНОДАТЕЛЬСТВО

Закон № 6698 о защите персональных данных и соответствующие административные положения.

3. ДАННЫЕ СПЕЦИАЛЬНОЙ КАТЕГОРИИ

В целях настоящего Регламента к особым категориям данных относятся следующие категории данных:

• Данные, касающиеся расы, этнического происхождения, политических взглядов, философских убеждений, религии, секты или других убеждений, внешнего вида и одежды, членства в ассоциациях, фондах или профсоюзах, состояния здоровья, сексуальной жизни, судимостей и мер безопасности, а также биометрические и генетические данные.

• Конфиденциальные данные, которые наша компания считает коммерческой
тайной. • Конфиденциальные данные в договорах, касающихся товаров, услуг и продукции.
Все данные определены.

• Конфиденциальные данные, касающиеся клиентов и поставщиков нашей компании.

Любой сотрудник, у которого возникают сомнения относительно того, относятся ли обрабатываемые данные к особой категории, обязан сообщить об этом руководителю соответствующего отдела и действовать в соответствии с его указаниями.

4. СООБРАЖЕНИЯ, КОТОРЫЕ СЛЕДУЕТ УЧИТЫВАТЬ ПРИ ПЕРЕДАЧЕ ДАННЫХ ОСНОВНЫЕ МОМЕНТЫ

4.1. При передаче персональных данных и конфиденциальных персональных данных каждый сотрудник должен проконсультироваться с соответствующим руководителем отдела для получения разрешения на передачу данных и предоставления инструкций.

4.2. Особые категории персональных данных и другие персональные данные должны передаваться только в той мере, в какой это абсолютно необходимо для надлежащего осуществления законной деятельности нашей Компании. Соответственно, перед каждой передачей данных следует заранее определить, необходима ли эта передача.

4.3. При взаимодействии с третьими сторонами следует учитывать наличие соглашений об обмене данными и дополнительных протоколов по защите персональных данных, подписанных с соответствующими сторонами. Кроме того, необходимо проверить наличие положений, касающихся предлагаемых методов передачи данных, и, если таковые имеются, следует проявлять осторожность при использовании предлагаемых методов.

4.4. Всегда следует проверять, предоставляется ли информация, выходящая за рамки необходимой для заявленной цели. Например, если запрашивается только раздел или конкретная часть документа, не следует отправлять весь документ или диаграмму.

4.5. Во всех случаях передачи персональных данных и информации, содержащей особые категории персональных данных, необходимо четко определить личность получателя и его полномочия на доступ к данным.

5. Методы передачи данных

Перед определением методов передачи данных следует учесть следующие моменты:

• Характер передаваемой информации, ее конфиденциальность, уровень секретности или потенциальная опасность. ценить

• Объем передаваемых данных •

Возможные убытки, которые могут понести заинтересованные лица в результате передачи данных потенциальные потери или трудности, которые могут остаться

• Последствия потери данных для нашей компании. • Информация и документы,

выходящие за рамки необходимого для заявленной цели, не должны передаваться. Все ненужные данные должны быть отредактированы или, при необходимости, полностью удалены перед передачей.

5.1. Передача данных по электронной почте

• Электронная почта не должна использоваться для передачи незашифрованных конфиденциальных данных, которые могут содержать личную информацию. Наши сотрудники должны понимать, что электронная почта не предназначена для прикрепления и передачи больших объемов данных.

• Наши сотрудники должны по возможности и целесообразности отдавать предпочтение альтернативным безопасным методам передачи конфиденциальных данных. В тех случаях, когда подходящая альтернатива недоступна, следует использовать дополнительные уровни защиты.

Например, следует использовать шифрование или требовать пароли и имена пользователей для доступа к конфиденциальным данным, которые необходимо отправить. При передаче имен пользователей и паролей следует использовать альтернативные методы, такие как почта, телефонные звонки на указанные номера или SMS-сообщения. • В электронных письмах следует

четко указывать на юридическую ответственность получателя, ошибочно получившего данные, и на то, что он должен делать с входящим письмом в случаях, когда получатель является не тем лицом. • В соответствующих случаях отправляемая информация должна быть вложена в запечатанные файлы.

Его следует отправить.

• Следует убедиться в точности информации, указанной в теме письма или сопроводительном сообщении. Не следует раскрывать в названии файла или теме письма все содержимое вложений или конфиденциальные персональные данные. • При отправке писем в компанию необходимо указывать соответствующую информацию о

конфиденциальности и безопасности.

Перевод необходимо осуществить, используя указанный адрес электронной почты.

5.2. Внутренний корпоративный портал

• Пользователям, которым необходимо скопировать или передать данные на съемный носитель, или которым необходимо отправить очень большой объем данных, следует обратиться за помощью в службу ИТ-поддержки компании.

• Доступ к порталу через файловый менеджер не допускается без предварительного разрешения службы ИТ-поддержки. • При загрузке данных на портал

убедитесь, что файлы имеют правильные имена и хранятся в соответствующих местах. Специализированные данные, которые необходимо загрузить на портал, не следует хранить в общедоступных местах.

• При загрузке данных в сеть компании следует использовать защищенный портал, соблюдая соответствующие процедуры.

• Каждый фрагмент данных, передаваемый в онлайн-образовательные ресурсы, должен быть зашифрован с помощью документа, защищенного паролем, или зашифрованного ZIP-файла.

5.3. Съемные устройства хранения данных (карта памяти, USB-накопитель и т. д.)

• Все данные, передаваемые через съемные носители, такие как портативные USB-накопители, должны быть зашифрованы. Зашифрованные портативные устройства хранения данных должны быть защищены надежными паролями. Если сам пароль необходимо раскрыть третьей стороне, эту информацию следует передавать альтернативными способами, такими как почта, телефон или SMS-сообщение.

• Пользователям, которым необходимо скопировать или передать данные на съемные носители, или которым необходимо отправить очень большой объем данных, следует обратиться за помощью в службу ИТ-поддержки компании.

• Право собственности на используемые съемные носители должно быть четко определено. Съемные носители должны быть возвращены владельцу после передачи данных, а переданные данные должны быть удалены с устройства хранения данных после использования.

• В случаях, когда получатель не является тем лицом, которому он адресован, и данные были переданы по ошибке, необходимо предоставить четкие инструкции относительно юридических обязанностей получателя и того, что делать с входящим электронным письмом.

• Раскрытие информации о содержимом зашифрованного файла в имени файла и прикрепленных сообщениях.
Этого делать не следует.

• Отправитель должен своевременно подтвердить успешность передачи данных и выдать соответствующее подтверждение.

Для этой цели могут подойти электронные письма, подтверждающие получение файла. • О любых проблемах следует сообщать непосредственным руководителям, а о любых потерянных или поврежденных данных необходимо немедленно сообщать сотруднику по защите данных/ответственному лицу.

5.4. Телефонные звонки

Поскольку телефонные разговоры могут прослушиваться, подслушиваться или прерываться (намеренно или случайно), следует принимать следующие меры предосторожности:

• Передача или обсуждение персональных данных по телефону запрещены без предварительной проверки личности и согласия получателя.

• При использовании автоответчика не оставляйте конфиденциальные или секретные сообщения и не указывайте личную информацию. Просто предоставьте средство связи и ожидайте, что получатель поговорит с вами лично.

• Во время прослушивания оставленных для вас голосовых сообщений другие люди могут подслушивать.
Будьте осторожны и не включайте аудиозапись на открытых пространствах, где существует риск несчастных случаев.

5.5. Передача данных почтой и курьерской службой

• Для передачи данных на физических носителях, таких как карты памяти или компакт-диски, следует использовать надежные почтовые службы. Предпочтение следует отдавать услугам экспресс-доставки и заказной почты, а не почтовым услугам первого или второго класса. При использовании почтовых служб, отличных от PTT (Турецкая почта), следует выбирать компании, предлагающие надежные курьерские услуги, требующие подписи при доставке.

• Получатель должен быть четко указан в почтовой накладной, а физическая упаковка должна быть надежно защищена от поломок или повреждений. • Получателей следует заранее уведомить о предполагаемой дате получения данных. Получатель должен подтвердить получение данных безопасным способом сразу после их получения. Отправитель, ответственный за передачу данных, обязан подтвердить безопасное получение данных.

5.6. Доставка лично в руки

К числу утвержденных способов передачи относятся личная передача и получение документов. Если получателю поручено получить передаваемые данные, его личность должна быть установлена заранее, и при передаче должны быть использованы соответствующие методы проверки личности, чтобы подтвердить, что получатель является предполагаемым лицом.

6. Отсутствующие данные

При обнаружении сотрудником факта потери данных он обязан немедленно сообщить об этом своему непосредственному руководителю и сотруднику по защите данных/координатору, а также незамедлительно выполнить процедуры, указанные в Положении о плане реагирования на утечку персональных данных.

При возникновении подозрения на несанкционированный доступ к конфиденциальным персональным данным следует немедленно уведомить правоохранительные органы.

7. Небрежность в процедурах передачи данных

Сотрудники, не соблюдающие положения настоящего Положения, могут быть признаны виновными в грубой халатности при исполнении служебных обязанностей, и их трудовые договоры могут быть расторгнуты. Нарушение защиты персональных данных может привести к тому, что наша компания потеряет с нами связь и понесет крупные штрафы.

Поэтому наши сотрудники должны проявлять максимальную осторожность при передаче конфиденциальных персональных данных. Это крайне важно. Действия, которые могут быть расценены как халатность и неправомерное поведение, включают в себя: несанкционированную передачу данных, ненадлежащее шифрование данных, отсутствие защиты с помощью сжатия и шифрования, использование нерегистрируемых или застрахованных почтовых услуг и т. д.