ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Документ №	KVKK_P1 ВЕРСИЯ 1.00
Дата пересмотра	-
Дата публикации	27.05.2024
Страница	13

Компания KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ПОЛИТИКА

1. ВВЕДЕНИЕ И ЦЕЛЬ

1.1. Настоящий документ подготовлен для изложения Рамочной политики информационной безопасности и защиты персональных данных компании Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi (далее именуемой Рамочной политикой), подробная информация о которой приведена ниже.

Контроллер данных	Компания Kardelen Paint and Chemical Industry Trade Limited: Alcı OSB
Адрес	Mah. 2036 Kad. No:7 Синкан/Анкара, Турция
Телефон	: +90 312 398 11 33
Почта	kvkk@kardelenboya.com.tr
Веб-сайт	: http://www.kardelenboya.com.tr/
Сфера деятельности	Производство красок

Данная рамочная политика содержит общий обзор применимых политик, правил, заявлений о раскрытии информации и руководящих принципов нашей компании в отношении информационной безопасности и конфиденциальности персональных данных, а также призвана продемонстрировать приверженность компании обучению и повышению осведомленности в этих областях.

1.2. Настоящая Рамочная Политика направлена на объединение необходимых и действующих условий для законной, безопасной, эффективной и действенной обработки всей информации и данных, полученных нашей Компанией. Обработка информации и данных имеет жизненно важное значение для ведения и управления повседневной деятельностью нашей Компании. Качество, планирование, оценка эффективности, охрана труда, страхование и финансовое управление услугами, предоставляемыми Компанией, во многом зависят от точных и надежных процессов сбора и обработки информации. Здоровое и надежное управление информацией требует открытого и эффективного управления и подотчетности, процессов управления, документированных политик и процедур, квалифицированного персонала и достаточных ресурсов. Соответственно, настоящая Рамочная Политика устанавливает условия, стандарты и передовые методы, которые будут действовать в области управления информационными ресурсами и законной обработки персональных данных.

1.3. Информационная безопасность и защита персональных данных являются важной обязанностью каждого сотрудника нашей компании. Каждый сотрудник несет ответственность за внедрение рабочих процедур компании и усвоение ее политики и правил работы.
Поэтому крайне важно, чтобы каждый из наших сотрудников был осведомлен о вопросах, изложенных в настоящем рамочном документе. От третьих лиц, использующих данные Компании, также ожидается соблюдение принципов, изложенных в настоящем рамочном документе.

1.4. Цель настоящей Рамочной политики — помочь нашей компании в выполнении следующих обязанностей:

• Соблюдение правовых, административных и договорных обязательств;
• Обеспечение надлежащего корпоративного управления; • Предоставление высококачественных услуг; • Защита финансовых ресурсов компании; • Планирование соответствующих процессов обеспечения непрерывности бизнеса; • Обеспечение постоянной безопасности операций с данными, находящихся под контролем компании. обеспечение и развитие.

1.5. Компания ежедневно осуществляет широкий спектр стандартных и специализированных мероприятий по сбору и обработке персональных данных, необходимых для предоставления услуг, обеспечения непрерывности коммерческих отношений и обязательств, а также гарантирования занятости своих сотрудников.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Настоящая Рамочная политика распространяется на все данные, хранящиеся в нашей Компании и обрабатываемые сторонами, осуществляющими обработку данных от имени Компании, включая данные, перечисленные ниже в качестве примеров, независимо от их формата:

• Хранится на настольных или портативных компьютерах и устройствах хранения данных.
• Обработка электронных данных;
• Передача данных по сетям;
• Информация, отправленная с использованием факса и аналогичных методов передачи данных; • Документы, хранящиеся на всех типах бумажных носителей; • Визуальные и фотоматериалы, включая микрофиши, слайды и записи с камер видеонаблюдения;
• Данные вербального общения, включая общение лицом к лицу, голосовые сообщения и записанные разговоры.

2.2. Стороны, перечисленные ниже, обязаны соблюдать процедуры и принципы, изложенные в настоящем Рамочном документе. Необходимо:

• Все сотрудники компании;
• Всем третьим сторонам, уполномоченным получать доступ к данным Компании, включая консультантов, поставщиков услуг и подрядчиков, а также посетителей.

2.3. Настоящая Рамочная политика состоит из двух частей. Первая часть описывает стратегию нашей Компании в отношении информационной безопасности и защиты персональных данных, а вторая часть...

В этом разделе описываются роли и обязанности соответствующих заинтересованных сторон в этом отношении, а также политика и программы обучения, которые будут реализованы в этой области.

2.4. Ниже приведена информация о том, как будут классифицироваться данные, находящиеся под контролем Компании. предоставляется:

(1) «Персональные данные» — это любая информация, относящаяся к идентифицированному или поддающемуся идентификации физическому лицу («субъект данных»); идентифицированное физическое лицо — это лицо, которое может быть прямо или косвенно идентифицировано по имени, идентификационному номеру, данным о местоположении, онлайн-идентификатору или одному или нескольким факторам, специфичным для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности соответствующего физического лица. При сборе, использовании и хранении персональных данных необходимо соблюдать процедуры и принципы, изложенные в Политике Компании по обработке и защите персональных данных;

(2) Данные, касающиеся расы, этнического происхождения, политических взглядов, философских убеждений, религии, секты или иных убеждений человека, внешности и одежды, членства в ассоциациях, фондах или профсоюзах, здоровья, сексуальной жизни, судимостей и мер безопасности, а также биометрические и генетические данные, являются особыми категориями персональных данных. Дополнительные условия и меры защиты для повышения безопасности при обработке особых категорий персональных данных указаны в Политике Компании по обработке и защите персональных данных и Политике безопасности данных.

(3) Следующие данные, за исключением персональных данных, являются корпоративными данными компании: будут называться данными:

(a) Плановые/административные или исследовательские данные, информация, защищенная законом о конфиденциальности в соответствии с соглашениями и положениями о конфиденциальности и т. д., которая имеет коммерческую защиту. Конфиденциальные корпоративные данные. Эти данные должны быть защищены с помощью самых современных мер безопасности;

(b) Неконфиденциальные данные, касающиеся компании, которые не были опубликованы и могут быть раскрыты в соответствии с требованиями законодательства, такими как Закон о свободе информации.

3. ЦЕЛЬ

3.1. Целью корпоративной стратегии нашей компании является обеспечение уверенности наших клиентов, партнеров и поставщиков в том, что данные обрабатываются и хранятся с должным учетом их ценности и рисков, а также обеспечение выполнения нашей компанией своих юридических обязанностей в области управления информацией, информационной безопасности и защиты персональных данных. Все заинтересованные стороны должны понимать важность надлежащего использования данных, их законного сбора и обработки, а также защиты от неправомерного использования.

3.2. Цель данной стратегии — обеспечить соблюдение нашей компанией правовых и этических норм, применимых к следующим областям:

• Законная обработка данных, касающихся идентифицированных или поддающихся идентификации лиц. его использование и обеспечение его безопасности;

• Доступ к данным должен осуществляться только в соответствии с законом.

• Передача персональных

данных физическим лицам; • Создание нормативно-правовой базы, применимой к управлению информацией; • Положения о регистрации, обмене и использовании персональных данных. Кодекс поведения в отношении получения явного согласия;

• Кодекс профессиональной этики и правил, принятый компанией.

В число

директив входят: • Взаимный обмен информацией и данными с третьими сторонами.

3.3. Стратегия направлена на поддержание надлежащих стандартов безопасности в области управления информацией, помимо высоких стандартов, ожидаемых от корпоративной идентичности компании, и на всестороннее формирование культуры защиты персональных данных во всей компании.

3.4. Ниже перечислены стратегические цели компании в отношении информационной безопасности и защиты персональных данных:

• Управление информацией должно поддерживать общую стратегию компании и связанные с ней подстратегии и программы трансформации бизнеса, а методы обеспечения информационной безопасности должны играть неотъемлемую роль в разработке и реализации этих стратегий и программ. • Необходимо создать необходимую инфраструктуру и процессы для

обеспечения того, чтобы нужная информация доходила до нужного человека в нужное время и для нужной цели, а также определить необходимую инфраструктуру и процессы для обеспечения того, чтобы эта информация доставлялась этичным, законным, эффективным и надлежащим образом;

• Разработка инновационных решений в области управления информацией с учетом трансформации бизнес-процессов; • Интеграция управления информацией в

административную деятельность компании путем внедрения комплексных изменений в поведении, направленных на признание информации как основополагающего актива;

• Конкретные аспекты управления информацией, касающиеся квалификации сотрудников и должностных инструкций. установление условий;

• Поощрение сотрудников к совместной работе для предотвращения излишних усилий и обеспечения более эффективного использования ресурсов; • Работа над обеспечением соблюдения

применимых стандартов в соответствии с правовыми, административными и договорными обязательствами и политиками;

• Выявление и управление информационными ресурсами внутри компании и создание системы управления информационными рисками, которая уравновешивает риски и возможности, применимые к этим информационным ресурсам;

• Обеспечение доверия всех заинтересованных сторон путем внедрения необходимых и соразмерных мер по применению передовых стандартов защиты информационных ресурсов;

• Обеспечение надлежащего обучения всех наших сотрудников и основных партнеров, повышение уровня осведомленности и гарантия того, что все данные и информация, обрабатываемые в компании, должным образом понимаются.

Создание подходящей культурной среды для решения проблем с чувством ответственности и долга.

4. ПОДХОД НАШЕЙ КОМПАНИИ

4.1. Информационная безопасность и конфиденциальность персональных данных полностью интегрированы в корпоративную деятельность нашей компании. В этом отношении учитываются четыре основных элемента деятельности компании:

- Человеческий фактор
- Процессы
- Информационные технологии

4.2. В деятельности по управлению, развитию и защите информации перечисленные выше факторы оцениваются с точки зрения того, как они способствуют достижению наших стратегических целей.

4.3. Планируется, что наши стратегические цели в области управления информацией будут достигаться посредством разрабатываемых политик. При разработке новых корпоративных программ и процессов каждый проект по управлению информацией будет определяться, внедряться и контролироваться в соответствии с подходами и административными правилами, описанными в настоящей Рамочной политике.

4.4. Ожидается, что реализация вышеупомянутой стратегии принесет следующие преимущества:

- Информация и данные, обрабатываемые внутри компании, обрабатываются согласованно и эффективно. управление;
- Более глубокое понимание соответствующего законодательства и уровня соблюдения его положений. возрастающий;
- События, влияющие на информационную безопасность и конфиденциальность персональных данных. значительно снизив его частоту;
- Время и усилия, которые сотрудникам приходится тратить на этот вопрос.
  - Сокращение; •

Повышение качества данных; • Четкое

определение обязанностей по управлению информацией и обеспечению безопасности.

быть представленным каким-либо образом;

- Эффективное управление рисками, угрожающими информационной и информационной безопасности;

4.5. Генеральный директор Компании отвечает за реализацию данной стратегии. Комитет по защите персональных данных, возглавляемый Генеральным директором, отвечает за мониторинг данной Рамочной политики и связанных с ней политик и директив в течение года, а также за отчетность о достигнутом прогрессе. Стратегия информационной безопасности и защиты персональных данных будет реализовываться посредством согласованных политик, программ развития и проектов. В конце каждого года Комитет по защите персональных данных будет проводить пересмотр стратегии.

Исходя из согласованных приоритетов и имеющихся ресурсов, генеральный директор утвердит программы развития, запланированные на следующий год. Генеральный директор утвердит программы развития, согласованные Комитетом по защите персональных данных.

4.6. Определения

4.6.1 ИСМС: Система управления информационной безопасностью.

4.6.2 Инвентаризация: Все информационные активы, имеющие важное значение для компании.

4.6.3 Высшее руководство: Это относится к высшему руководству компании.

4.6.4 Ноу-хау: Способность что-либо делать.

4.6.5 Конфиденциальная информация: Информация, как и все другие корпоративные и деловые активы, является ценным активом для бизнеса и, следовательно, должна надлежащим образом защищаться. Внутри компании ноу-хау, процессы, формулы, методы и технологии, данные о клиентах, маркетинговая и сбытовая информация, информация о персонале, коммерческая, промышленная и технологическая информация, а также секреты считаются КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ.

4.6.6 Конфиденциальность: Это относится к ограничению доступа к содержимому информации только для тех, кто имеет право просматривать эту информацию/данные. (Пример: Зашифрованная отправка электронных писем предотвращает чтение писем посторонними лицами, даже если они будут перехвачены — заказная электронная почта — KEP)

4.6.7 Целостность: Это означает обеспечение возможности обнаружения несанкционированных или случайных изменений, удалений или добавлений информации, а также гарантирование отслеживаемости. (Пример: Хранение данных в базе данных вместе со сводной информацией — электронная подпись — мобильная подпись)

4.6.8 Доступность/Наличие: Это означает, что актив должен быть готов к использованию в любое время, когда это необходимо. Другими словами, системы должны быть постоянно доступны, данные в системах не должны быть потеряны, и к ним должен быть обеспечен постоянный доступ. (Пример: использование источников бесперебойного питания и резервных источников питания в корпусах серверов для защиты от колебаний напряжения в сети и отключений электроэнергии — ИБП).

4.6.9 Информационные активы: Это активы, принадлежащие Компании и необходимые для бесперебойного функционирования ее деятельности. В рамках процессов, охватываемых настоящей политикой, к информационным активам относятся следующие:

- Все виды информации, представленные в бумажном, электронном, визуальном или аудиоформате, и данные,
- Любое программное обеспечение, используемое для доступа к информации и ее изменения, и аппаратное обеспечение,
- Сети, обеспечивающие передачу информации,

• Удобства и приватные зоны,

• Отделы, подразделения, команды и сотрудники,

• Партнеры по решениям,

• Это услуги, продукты или предложения, предоставляемые третьими сторонами.

4.7. Организационная схема, включенная в приложение к настоящей Рамочной политике, определяет участников и их роли в управлении информацией внутри Компании.

4.7.1 Ответственность руководства

- Руководство компании обязуется соблюдать разработанную, внедренную и подлежащую исполнению Систему информационной безопасности и защиты персональных данных, выделять необходимые ресурсы для эффективного функционирования системы и обеспечивать понимание системы всеми сотрудниками. Генеральный директор, как правило, отвечает за оценку и снижение рисков информационной безопасности и обеспечивает распространение соответствующих политик и информации среди всех сотрудников компании, которым это необходимо знать. Риски информационной безопасности будут рассматриваться аналогично другим финансовым, юридическим и репутационным рискам.

- В процессе создания системы информационной безопасности и защиты персональных данных назначается сотрудник по взаимодействию с заинтересованными сторонами на основании письменного документа. При необходимости документ может быть пересмотрен высшим руководством, и назначение может быть произведено повторно.

- Руководители высшего звена помогают подчиненным, распределяя обязанности и подавая пример в вопросах безопасности. Такой подход, начиная с самых высоких уровней и доводя его до самых низших должностей, имеет важное значение.

Поэтому все руководители призывают своих сотрудников, как в письменной, так и в устной форме, следовать инструкциям по технике безопасности и участвовать в мероприятиях, связанных с безопасностью.

- Высшее руководство выделило бюджет, необходимый для проведения комплексных мероприятий по обеспечению информационной безопасности.

Оно творит.

Сотрудник по связям с данными отвечает перед назначенным высшим руководством за подписание соглашений об обмене и обработке данных, а также дополнительных протоколов с соответствующими заинтересованными сторонами, а также за подготовку других соглашений и протоколов, касающихся доступа к данным и их передачи, необходимых в рамках деятельности компании.

4.7.2. Контактное лицо по данным

Специалист по связям с данными отвечает за разработку и реализацию необходимой корпоративной стратегии, концепции и программ для защиты информационных активов и систем компании. Его обязанности в этом отношении перечислены ниже:

- Планирование системы информационной безопасности и защиты персональных данных является приемлемым. определение уровня риска, определение методологии оценки риска,

- Предоставление необходимых ресурсов для поддержки и дополнительных мероприятий по созданию системы информационной безопасности и защиты персональных данных, обеспечение/улучшение возможностей пользователей и повышение осведомленности, проведение обучения, обеспечение коммуникации и предоставление необходимой документации.

- Внедрение и управление приложениями систем информационной безопасности и защиты персональных данных, обеспечение непрерывности оценок, улучшений и анализа рисков.

- Внутренние аудиты, совещания по определению целей и анализу работы руководства, а также информационная безопасность. а также оценка системы защиты персональных данных и мер по ее контролю.

- Сохранение существующей структуры и обеспечение непрерывного совершенствования системы информационной безопасности и защиты персональных данных.

4.7.3 Руководители отделов

- Проведение инвентаризации активов и анализа рисков, связанных с подразделениями.

- Сотрудник, ответственный за обработку данных, обязан проводить оценку рисков всякий раз, когда происходят изменения в информационных активах, находящихся в его ведении, которые могут повлиять на риски информационной безопасности. информация,

- Сотрудники, находящиеся под его/ее руководством, обязаны соблюдать корпоративные правила и положения компании. обеспечение его функционирования в соответствии с установленными процедурами.

- Повышение осведомленности и обеспечение коммуникации в рамках системы управления информационной безопасностью (СУИБ) в отношении соответствующих департаментов. Предоставление требований к документации,

- В системах управления информационной безопасностью (СУИБ) это означает поддержание существующей структуры и обеспечение непрерывного совершенствования. ответственный.

- Руководители отделов несут ответственность за оценку аспектов управления информацией в рамках рабочих процессов своих отделов и в деятельности, осуществляемой в сотрудничестве с заинтересованными сторонами. Для получения информации о конкретных обязанностях в области информационной безопасности, пожалуйста, ознакомьтесь с Политикой информационной безопасности.

4.7.4 Ответственность всех сотрудников

- Они несут ответственность за выполнение своей работы в соответствии с целями, политиками и документами системы управления информационной безопасностью.

- Мониторинг целей информационной безопасности, относящихся к собственному подразделению, и содействие достижению этих целей.

- Любые обнаруженные или предполагаемые проблемы информационной безопасности в системах или сервисах. от выявления и сообщения о любых недостатках или нарушениях,

- Помимо договоров на оказание услуг (консультации и т. д.) с третьими сторонами, за которые Заказчик не несет ответственности, Заказчик отвечает за заключение соглашений о конфиденциальности и обеспечение соблюдения требований информационной безопасности.

- Все сотрудники компании и третьи лица, уполномоченные получать доступ к информационным активам компании, обязаны соблюдать законы и нормативные акты, осознавая свою личную ответственность за управление информацией. Все сотрудники должны придерживаться установленных компанией правил, процедур и руководящих принципов, а также участвовать в обучении и мероприятиях, связанных с управлением информацией.

5. ОБЩИЕ ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Сотрудники компании и третьи стороны обязаны быть осведомлены о деталях и процедурах, касающихся требований и правил информационной безопасности, изложенных в настоящей Рамочной политике, и выполнять свою работу в соответствии с этими правилами.

5.2. Если не указано иное, настоящие правила и положения должны соблюдаться в отношении всей информации, хранящейся и обрабатываемой в печатной или электронной форме, а также в отношении использования всех информационных систем.

5.3. Система информационной безопасности и защиты персональных данных построена и функционирует на основе Закона Турции о защите персональных данных (KVKK), GDPR и стандарта TS ISO/IEC 27001 «Методы обеспечения безопасности информационных технологий и требования к системам управления информационной безопасностью».

5.4. Внедрение, функционирование и совершенствование Системы информационной безопасности и защиты персональных данных осуществляется при участии соответствующих сторон. Ответственный за обновление соответствующих документов отвечает сотрудник, ответственный за защиту данных.
Это их ответственность.

5.5. Если иное не предусмотрено законом или договором, информационные системы и инфраструктура, предоставляемые компанией сотрудникам или третьим лицам, а также вся информация, документы и продукция, созданные с использованием этих систем, принадлежат компании Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi.

5.6. Соглашения о конфиденциальности подписываются с сотрудниками, консультантами, поставщиками услуг (охрана, транспорт, кейтеринг, клининговые компании и т. д.), поставщиками и стажерами.

5.7. Информация, используемая в процессах найма, смены работы и увольнения.
Определены и внедрены меры безопасности.

5.8. Для действующих и вновь принятых на работу сотрудников регулярно проводятся обучающие занятия, направленные на повышение осведомленности сотрудников в вопросах информационной безопасности и предоставление им возможности вносить свой вклад в функционирование системы.

5.9. Сообщается обо всех фактических или предполагаемых нарушениях информационной безопасности; выявляются нарушения, вызвавшие эти нарушения, определяются их первопричины и принимаются меры для предотвращения их повторения.

5.10. Создается перечень информационных активов, и право собственности на них определяется в соответствии с потребностями управления информационной безопасностью.

5.11. Персональные и корпоративные данные классифицируются, и обеспечивается безопасность данных в каждой категории. Определяются потребности и правила использования.

5.12. Физическая безопасность в соответствии с потребностями активов, хранящихся в защищенных зонах. Применяются меры контроля.

5.13. Раскрытие информационных активов компании как внутри, так и за пределами организации. Для противодействия физическим угрозам разрабатываются и внедряются необходимые меры контроля и политики.

5.14. Разрабатываются и внедряются процедуры и инструкции, касающиеся управления мощностями, взаимоотношений с третьими сторонами, резервного копирования, приемки системы и других процессов обеспечения безопасности.

5.15. Настройки для генерации журналов аудита для сетевых устройств, операционных систем, серверов и приложений корректируются в соответствии с потребностями безопасности соответствующих систем. Аудиторские записи защищены от несанкционированного доступа.

5.16. Права доступа назначаются по мере необходимости. Для контроля доступа используются максимально безопасные технологии и методы.

5.17. Требования к безопасности определяются в процессе закупки и разработки системы. В ходе приемки или испытаний проверяется соответствие требованиям безопасности.

5.18. Планы обеспечения непрерывности работы критически важной инфраструктуры разрабатываются, поддерживаются и отрабатываются на практике.

5.19. Разработаны процессы, обеспечивающие соблюдение законов, внутренних правил и процедур, а также технических стандартов безопасности; соблюдение обеспечивается посредством непрерывного и периодического мониторинга и аудита.

6. ПОЛИТИКА, КОТОРАЯ ДОЛЖНА БЫТЬ РАЗРАБОТАНА В РАМКАХ ПОЛИТИК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. В рамках Политики информационной безопасности и защиты персональных данных предусмотрены следующие положения, определяющие политику и кодексы поведения:

ССЫЛКА НА ТИП ДОКУМЕНТА	ЧИСЛО	ЗАГОЛОВОК
ПОЛИТИКА	KVKK_P1	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЛИЧНОСТЬ ПОЛИТИКА РАМКИ ДАННЫХ
ПОЛИТИКА	KVKK_P2	ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ПОЛИТИКА ОБРАБОТКИ
ПОЛИТИКА	KVKK_P3	ПОЛИТИКА ХРАНЕНИЯ И УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

ПОЛИТИКА	KVKK_P4	Персональные данные, относящиеся к сотрудникам. ДАННЫЕ ЗАЩИТА ПОЛИТИКА
ПОЛИТИКА	KVKK_P5	ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПОЛИТИКА	KVKK_P6	ИНФОРМАЦИЯ И КОММУНИКАЦИЯ ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ПОЛИТИКА
ПОЛИТИКА	KBKK_П7	ПОЛИТИКА КОНТРОЛЯ ДОСТУПА
ПОЛИТИКА	KVKK_P8	СИСТЕМЫ ВНУТРЕННЕГО ВИДЕОНАБЛЮДЕНИЯ ПОЛИТИКА
ПОЛИТИКА	KVKK_P9	ПРИНЯТИЕ ИНТЕРНЕТА И ИНСТРУМЕНТОВ ЭЛЕКТРОННОЙ КОММУНИКАЦИИ это можно сделать ИСПОЛЬЗОВАНИЕ ПРОЦЕДУРЫ И ПРИНЦИПЫ, ОТНОСЯЩИЕСЯ К ПОЛИТИЧЕСКИЕ
ПОЛИТИКА	KVKK_P10	ПОЛИТИКА В ОТНОШЕНИИ ВИДЕОРЕГИСТРАЦИЙ В АВТОМОБИЛЕ
ПРАВИЛА	KVKK_Y1	СУБЪЕКТЫ ДАННЫХ В ОТНОШЕНИИ ИХ ПРОСЬБ ДОЛЖНО БЫТЬ ПРЕДОСТАВЛЕНО ПРИНЦИПЫ И ПРОЦЕДУРЫ ОТВЕТОВ ПРАВИЛА, КАСАЮЩИЕСЯ
ПРАВИЛА	KVKK_Y2	ПЛАН РЕАГИРОВАНИЯ НА УТЕЧКУ ДАННЫХ РЕГУЛИРОВАНИЕ
ПРАВИЛА	KVKK_Y3	ВЛИЯНИЕ НА ЗАЩИТУ ДАННЫХ ПРОЦЕДУРА ОЦЕНКИ И О ЕГО ПРИНЦИПАХ ПРАВИЛА
ПРАВИЛА	KVKK_Y4	ЭЛЕКТРОННАЯ СВЯЗЬ И ЭЛЕКТРОННЫЕ ДАННЫЕ ОБ ИНСПЕКЦИИ ПРАВИЛА
ПРАВИЛА	KVKK_Y5	ЭЛЕКТРОННЫЕ СООБЩЕНИЯ ПОРЯДОК ИСПОЛЬЗОВАНИЯ И ПОЛОЖЕНИЯ О ЕЕ ПРИНЦИПАХ
ПРАВИЛА	KVKK_Y6	КАМЕРА ЗАЩИТНОЙ СИСТЕМЫ ПОРЯДОК ИСПОЛЬЗОВАНИЯ СИСТЕМ И О ЕГО ПРИНЦИПАХ ПРАВИЛА
ПРАВИЛА	KVKK_Y7	ПАРОЛИ ПОЛЬЗОВАТЕЛЕЙ ИДЕНТИФИКАЦИЯ, ИСПОЛЬЗОВАНИЕ И ПРОЦЕДУРЫ ПО ЕГО ЗАЩИТЕ О ПРИНЦИПАХ ПРАВИЛА
ПРАВИЛА	KVKK_Y8	ПРОЦЕДУРА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ И О ЕГО ПРИНЦИПАХ ПРАВИЛА
ТЕКСТ ЗАЩИТЫ ДАННЫХ KVKK_A1		ДЕЙСТВИТЕЛЬНО ДЛЯ ПОДАЧИ ЗАЯВОК НА РАБОТУ. Информационный текст GDPR
ТЕКСТ ЗАЩИТЫ ДАННЫХ KVKK_A2		ИНТЕРНЕТ ФАЙЛЫ COOKIE САЙТА ИСПОЛЬЗОВАНИЕ О ИНФОРМАЦИОННЫЙ ТЕКСТ

ТЕКСТ ЗАЩИТЫ ДАННЫХ KVKK_A3		СИСТЕМЫ ВНУТРЕННЕГО ВИДЕОНАБЛЮДЕНИЯ ИНФОРМАЦИОННЫЙ ТЕКСТ
ТЕКСТ ЗАЩИТЫ ДАННЫХ KVKK_A4		Информационный текст о Законе о защите персональных данных (KBKK)
ТЕКСТ ЗАЩИТЫ ДАННЫХ KVKK_A5		ОСВЕЩЕНИЕ ВЕБ-САЙТА ТЕКСТ
ТЕКСТ ЗАЩИТЫ ДАННЫХ KVKK_A6		ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ О ПОДРЯДЧИКЕ ИНФОРМАЦИОННЫЙ ТЕКСТ
ТЕКСТ ЗАЩИТЫ ДАННЫХ KVKK_A7		ИНФОРМАЦИЯ ДЛЯ ПОСЕТИТЕЛЕЙ
ФОРМА	KVKK_F1	ВЛИЯНИЕ НА ЗАЩИТУ ДАННЫХ ФОРМА ОЦЕНКИ
СОГЛАШЕНИЕ	KVKK_S1	ПЕРСОНАЛЬНЫЕ ДАННЫЕ ПРИЛОЖЕНИЕ ОТНОСИТЕЛЬНО ЕГО ЗАЩИТЫ ПРОТОКОЛ

6.2. Разработка политики

6.2.1. Комитет по защите персональных данных рассматривает все политики управления информационной безопасностью и, при необходимости, представляет свои рекомендации по изменениям высшему руководству. Все установленные политики и соответствующие обновления доводятся до сведения сотрудников через корпоративный портал или интернет.

6.2.2. Политика пересматривается ежегодно и обновляется по мере необходимости, а для устранения недостатков могут быть разработаны новые положения. В соответствующих случаях эти положения рассматриваются в совокупности с трудовым договором работника.

6.2.3. Политики, разрабатываемые в рамках настоящей Рамочной политики, будут определять сферу действия и цели, а также предоставлять основу для управления информационной безопасностью, определяющую обязанности персонала и других заинтересованных сторон. Компания обязуется принимать необходимые меры для обеспечения информированности своих сотрудников и сторон, с которыми она имеет деловые отношения, о целях Компании и обязанностях, ожидаемых от соответствующих заинтересованных сторон в достижении этих целей. В этом отношении разработанные Политики и Положения играют ключевую роль в информировании сотрудников и деловых партнеров об ожидаемых от ни

6.3. Обучение и развитие

6.3.1. Программы обучения и повышения квалификации в области управления информационной безопасностью имеют важное значение для улучшения и совершенствования знаний и навыков персонала всей компании в области управления информационной безопасностью.

6.3.2. Обучение управлению информационной безопасностью должно включать темы, выходящие за рамки базового понимания вопросов конфиденциальности и безопасности, с целью разработки и мониторинга передовых методов. Персонал должен понимать ценность информации и свои обязанности, включая качество данных, информационную безопасность, управление документацией, конфиденциальность и т. д.

7. Мониторинг соблюдения рамочной политики.

7.1. Комитет по защите персональных данных отвечает за обеспечение соблюдения настоящей Рамочной политики, а также за пересмотр и обновление каждой соответствующей политики.

7.2. Политики и процедуры следует пересматривать не реже одного раза в год. Кроме того, их следует пересматривать после любых изменений, затрагивающих структуру системы или оценку рисков, а все необходимые изменения должны быть утверждены высшим руководством и зарегистрированы как новая версия. Каждая редакция должна быть опубликована в доступной для всех пользователей форме.

7.3. Совещания по анализу эффективности работы руководства организуются сотрудником по связям с данными и проводятся с участием высшего руководства и руководителей отделов. Эти совещания, на которых оценивается пригодность и эффективность системы управления информационной безопасностью, проводятся не реже одного раза в год.

8. НАРУШЕНИЕ ПОЛИТИКИ И САНКЦИЙ

В случае установления факта несоблюдения Политики и стандартов информационной безопасности и защиты персональных данных, к сотрудникам, ответственным за это нарушение, будут применены санкции, указанные в соответствующих пунктах договоров, которые также распространяются на третьих лиц, в соответствии с Дисциплинарной директивой и процедурой.