ВЛИЯНИЕ НА ЗАЩИТУ ДАННЫХ

ПРОЦЕДУРА ОЦЕНКИ И О ЕГО ПРИНЦИПАХ ПРАВИЛА

KVKK_Y3 ВЕРСИЯ 1.00

Компания KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED

Оценка воздействия на защиту данных (DPIA) ПРАВИЛА ПРОЦЕДУР И ПРИНЦИПОВ

1. ВВЕДЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее Положение о процедурах и принципах оценки воздействия на защиту данных (далее именуемое «Положение») следует оценивать совместно с Политикой информационной безопасности нашей Компании, Политикой защиты персональных данных и Рамочной политикой.

1.2. Настоящий Регламент регулирует процедуры и принципы, которым следует следовать, когда наша Компания, как контролер данных, обязана проводить оценку воздействия планируемых операций по обработке данных на защиту персональных данных до начала обработки (статья 35 GDPR), или когда владельцы информационных активов проводят оценку воздействия на защиту данных в ходе ежегодного обзора контролируемых ими информационных активов, особенно когда используются новые технологии в области информационно-коммуникационных технологий или в общем коммерческом использовании, и когда определенный вид обработки данных может представлять высокий риск для прав и свобод физических лиц, с учетом характера, масштаба, контекста и целей обработки данных.

1.3. Определения: Для целей настоящего положения под информационными активами понимаются активы, принадлежащие компании Kardelen Boya, которые необходимы для бесперебойного ведения ее деятельности и которые, следовательно, она обязана защищать.

1.4. Владелец информационного актива: руководитель бизнес-подразделения, в котором используется соответствующий актив.

2. Оценка воздействия на защиту данных

2.1. Сотрудники, назначенные владельцами информационных активов, несут ответственность за управление находящимися в их распоряжении информационными активами в соответствии с обязанностями, описанными в Рамочной политике.

2.2. Владельцы информационных активов обязаны проводить оценку воздействия не реже одного раза в год, и особенно при существенных изменениях в информационных активах, методах их хранения и обработки, а также при изменениях в законодательных нормах или политиках, предусматривающих изменения в персональных данных, хранящихся в информационных активах, они должны проводить оценку воздействия до внедрения каких-либо изменений.

2.3. Владельцы информационных активов должны обеспечить соответствие безопасности контролируемых ими активов следующим условиям, изложенным в Политике информационной безопасности Компании:

• Все пользователи должны надлежащим образом убедиться, что у них есть доступ к информации, прежде чем использовать её. Они должны быть авторизованы.

• Разумное вознаграждение, соответствующее ценности и/или конфиденциальности информационного актива.

Необходимо обеспечить определенный уровень безопасности.

• Пользователи обязаны сообщать о любых инцидентах, приводящих или способных привести к нарушению безопасности данных, сотруднику по вопросам защиты данных и ИТ-менеджеру. Пострадавшие пользователи также должны незамедлительно уведомить группу ИТ-поддержки, руководителей своих отделов или высшее руководство компании о нарушении.

• Пользователи обязаны проводить оценку воздействия на защиту данных (Data Protection Impact Assessment, DIA) в отношении своих активов в рамках ежегодного пересмотра инвентаризации информационных активов.

2.3.1. Каждый владелец информационного актива обязан прилагать разумные усилия для обеспечения того, чтобы все материалы, находящиеся в его распоряжении, постоянно соответствовали следующим требованиям:

• Собранные данные должны быть предоставлены на законных основаниях.

• Необходимо соблюдать Условия использования ИТ-ресурсов, изложенные в Разделе 11 Политики информационной безопасности компании.

• Собранные данные не должны содержать ссылки на незаконные материалы и не должны содержать контент, противоречащий Условиям использования компанией информационных и коммуникационных инструментов.

• За исключением случаев, одобренных руководителем соответствующего отдела, запрещается публиковать рекламные материалы или комментарии о товарах, продукции или услугах от имени Компании.

• За исключением случаев, одобренных соответствующим руководителем отдела, владельцем информационных активов или компанией, товариществом, консорциумом или консалтинговой фирмой любого другого лица, любая информация и/или данные, содержащие рекламные материалы или комментарии об их «частной» деятельности, не должны включаться.

2.3.2. Информация, принадлежащая любому физическому лицу, которая включена в информационные активы компании и данные:

• Оно не должно содержать товарный знак, логотип, фирменный бланк и т. д. компании.

- Сохраняемые материалы должны быть непосредственно связаны с разрешением владельца информационных активов на использование ИТ-активов компании или иметь к нему отношение.

- Независимо от того, как на них ссылаются, соответствующие политики и правила компании, а также способ представления информации, хранящейся у отдельных лиц, ни в коем случае не должны толковаться как подразумевающие, что Компания принимает на себя какую-либо ответственность за эту информацию, хранящуюся у отдельных лиц, или одобряет какие-либо материалы или мнения, содержащиеся в ней.

В отношении всей информации, хранящейся у отдельных лиц, на экране должно отображаться заверенное уведомление, указывающее на то, что данная информация не была официально опубликована Компанией.

2.4. Весь персонал несет ответственность за соблюдение передовых методов обеспечения информационной безопасности для гарантирования надлежащей защиты информации, хранящейся в Компании, независимо от формата ее хранения. Все руководители отделов несут ответственность за контроль за соблюдением правил информационной безопасности в своих отделах в рамках своих управленческих обязанностей. В рамках этого процесса руководители отделов проводят проверку активов, хранящихся в их отделах, и обязаны внедрять необходимые меры и средства контроля для обеспечения того, чтобы инвентаризация информационных активов Компании точно отражала все управляемые активы.

2.5. Инвентаризация информационных активов помогает соответствующим отделам определить, какая конкретная ИТ-поддержка необходима для конкретных информационных активов с точки зрения безопасности информационно-коммуникационных технологий и управления ИТ-активами, а также в проведении мероприятий по обеспечению информационной безопасности. Хотя инвентаризацией информационных активов управляет ИТ-менеджер, необходимо принимать соответствующие меры предосторожности, учитывая безопасность записей и активов, хранящихся в бумажном формате.

2.6. Информационные активы следует идентифицировать с помощью логических связей и методов сбора. Например, информация, собранная для исследования в области охраны труда и техники безопасности, может храниться на различных носителях, включая несколько ноутбуков, группу жестких дисков и USB-накопители. В этом случае необходимо составить запись, описывающую каждый носитель и способы его защиты.

2.7. Каждый соответствующий отдел должен задекларировать имеющиеся у него информационные активы и обеспечить их учет в инвентаризационном списке. Каждая дополнительная система хранения данных, приобретенная локально для целей цифрового/документационного хранения, должна быть зарегистрирована как актив «Система, используемая отделом». В случае сомнений относительно необходимости учета дополнительных информационных активов следует обратиться в службу ИТ-поддержки. Системы облачного хранения данных и системы бумажного документооборота также должны быть определены как информационные активы и зарегистрированы в инвентаризационном списке.

2.8. При анализе информационных ресурсов своих подразделений руководителям подразделений следует учитывать следующее:

• Есть ли какие-либо информационные активы, которые необходимо добавить в инвентаризацию?

• Любые информационные активы, которые не используются и должны быть исключены из инвентаризации. Это возможно?

• Произошли ли изменения в использовании информационных активов, которые потребуют обновления записей в реестре информационных активов?

• Предусмотрены ли какие-либо изменения в политике или законодательных нормах, которые влекут за собой изменение порядка сбора и обработки информационных ресурсов, используемых департаментом?

2.9. Следует признать, что руководители отделов не обладают исчерпывающей информацией обо всех данных, с которыми работают сотрудники их отделов, или обо всех элементах, в которых эта информация хранится. Рекомендуется, чтобы при заполнении отчета об информационных активах отделы уделяли широкое внимание основным рискам, связанным с информацией, хранящейся в отделе, и местом ее хранения. Отделам может быть полезно сосредоточиться на передаче данных, особенно если данные являются конфиденциальными или передаются за пределы колледжа. Для получения дополнительной информации обратитесь в группу по информационной безопасности.

3. СТРУКТУРА ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ АКТИВОВ

Доменное имя	Пояснения
Владелец информационных активов	Кто несет ответственность за информацию, хранящуюся в этом массиве данных, и кто является контактным лицом/ответственным за запросы, касающиеся этого массива данных?
Менеджер информационных активов	Роль менеджера информационных активов определена в документе «Структура системы управления информационной безопасностью» и может быть описана как роль наиболее уполномоченного лица, которое ежедневно использует информационные активы.
Название информационного актива	Конкретное название, присвоенное информационному активу.
Определение информационного актива	Предоставьте краткое описание информационного актива. По возможности, включите краткую информацию о том, какие данные будут храниться в этом активе.
Текущий статус актива отображается только в инвентаризации информационных активов — временный, утвержденный, неактивный и т. д.	
Классификация	• Содержит ли информационный ресурс данные особых категорий? Какие риски связаны с этими данными? Какие меры принимаются для устранения или смягчения этих рисков? К особой категории данных относятся следующие: о Данные, относящиеся к управлению компанией или исследованиям, которые считаются коммерчески конфиденциальными.

	данные. Это относится к «данным, касающимся расы, этнического происхождения, политических взглядов, философских убеждений, религии, секты или иных убеждений, внешнего вида и одежды, членства в ассоциациях, фондах или профсоюзах, состояния здоровья, сексуальной жизни, судимостей и мер безопасности, а также биометрическим и генетическим данным», как указано в статье 6 Закона № 6698. То есть, индивидуальные финансовые данные; то есть, данные, относящиеся к исследовательским Разработка работам, заказанным компанией. В эту категорию следует также отнести персональные данные, не указанные выше, но раскрытие которых может причинить вред или ущерб репутации соответствующих лиц.
Где будет храниться актив Тип среды	Электронный, ручной или и тот, и другой.
Правовая основа	Каковы правовые основания для обработки и/или хранения соответствующих данных? В соответствии с Законом № 6698, для законной обработки персональных данных необходимо учитывать законные основания для обработки данных, которые могут быть использованы контролерами данных.
С точки зрения организации рабочего процесса Его важность	Жизненно важное значение информационного актива для рабочего процесса компании и уровень негативных последствий, которые возникнут в случае его утраты или нарушения конфиденциальности.
Местонахождение информационного актива. Где физически хранится информационный актив? Например, на локальных компьютерах, в центральной системе, на портале или в другом месте, помимо сервера?	
Добавление информационного актива Сторона	Лицо, внесшее соответствующую запись в реестр информационных активов. Кто это?
Ожидаемое хранение Продолжительность	Как долго информационный актив будет храниться в инвентаре? Каков предусмотренный порядок определения того, что информация больше не нужна для деятельности Компании, и ее безопасного уничтожения? Пожалуйста, ознакомьтесь с Политикой Компании по хранению и уничтожению данных относительно сроков, по истечении которых данные должны быть уничтожены.
Самая старая запись	Дата самой старой записи, которая не должна попадать в текущий диапазон сроков хранения.
Последняя запись	Дата последней записи для информационных активов, которые больше не обновляются.

Должностные лица, назначенные владельцами информационных активов, также должны учитывать следующее:

• Ответственное подразделение: Какое подразделение отвечает за рассматриваемый информационный актив? (Обычно это подразделение, ответственное за «владельца актива»)

• Какие подразделения и/или сотрудники будут иметь доступ к информационному ресурсу? Пожалуйста, укажите группы лиц, которые, как ожидается, будут иметь доступ к соответствующему информационному ресурсу. Например, сотрудники, назначенные в определенную команду, или все сотрудники компании. Кроме того, следует четко указать третьих лиц, не являющихся сотрудниками компании, но которые, как ожидается, будут иметь доступ к соответствующему информационному ресурсу.

• Как будет обеспечена безопасность информационного актива? Кратко опишите меры, принимаемые для обеспечения безопасности информационного актива. Например, защита паролем. Хранятся ли записи, содержащие конфиденциальные персональные данные, в бумажном формате в запертой системе хранения документов? Как обслуживаются замки? Предупреждение: Ни при каких обстоятельствах не разглашайте место хранения паролей или замков! • Резервное копирование, отказоустойчивость и аварийное восстановление:

Какие меры принимаются для восстановления данных и/или поддержания функциональности и доступности данных в случае потери данных или нарушения безопасности данных/систем, а также в случае стихийных бедствий, землетрясений и т. д.?