EuroChem

Политика защиты персональных данных
Документ № C6.PLC.01

Версия 1.0
25 апреля 2018

Юридические уведомления

Краткая справка

НАЗВАНИЕ	Политика защиты персональных данных
ИДЕНТИФИКАЦИОННЫЙ НОМЕР	C6.PLC.01
КОНТРОЛЕР ПРОЦЕССА	А.А. Ильин, Chief Financial Officer, EuroChem Group
ОТВЕТСТВЕННЫЙ ЗА ПРОЦЕСС	В.В. Сиднев, General Counsel, EuroChem Group
РАЗРАБОТЧИК	Е.В. Холманских, Chief Compliance Officer, EuroChem Group
ВЕРСИЯ	1.0
ДАТА ВСТУПЛЕНИЯ В СИЛУ	25.05.2018
ДАТА ОДОБРЕНИЯ	24.04.2018

Лист регистрации изменений

Версия	Дата вступления в силу	Цель	Сведения о внесении изменений
<версия>	<дата вступления в силу>		N/A
1.0	25.05.2018	…	…

Содержание

1. Термины и определения

При отсутствии противоположных указаний, термины, которым дано определение (или конкретное толкование) в Кодексе поведения и Политике по вопросам обеспечения выполнения нормативных требований (комплаенс), имеют то же значение (или подлежат аналогичной интерпретации) в настоящей Политике защиты персональных данных (“Политика”).

Кроме того, в настоящем документе применяются следующие определения:

Термин	Определение
“Персональные данные”	обозначает любую информацию, относящуюся к идентифицированному Субъекту данных; существует широкий набор идентификационных признаков, включая имя физического лица, (рабочий) телефонный номер, (рабочий) адрес электронной почты, идентификационный номер, данные о местонахождении, онлайн-идентификатор и т.п.
“ Данные ограниченного доступа”	обозначает Персональные данные, отражающие расовое или этническое происхождение, политические взгляды, религиозные или философские воззрения, членство в профсоюзных организациях, а также обработку генетических данных, биометрических данных для целей уникальной идентификации физического лица, данных, касающихся здоровья, частной жизни или сексуальной ориентации физического лица.
“Контролер данных” или “Контролер”	обозначает физическое или юридическое лицо, государственный орган, учреждение или иную организацию, которые, самостоятельно или совместно с другими лицами, определяют цели и средства обработки персональных данных.
“Центр обработки данных”	физическое или юридическое лицо, обрабатывающее персональные данные от имени Контролера.
“Субъект данных”	обозначает любое живущее физическое лицо, являющееся субъектом Персональных данных, которые содержатся Группой.
“Обработка”	обозначает любую операцию или серию операций с Персональными данными или комплектами персональных данных, в том числе с помощью автоматических средств, например, сбор, регистрацию, организацию, структурирование, хранение, адаптацию или изменение, извлечение, ознакомление, использование, раскрытие путем передачи, распространение или предоставление иным образом, приспособление или объединение, ограничение, удаление или уничтожение.
“Нарушение обработки Персональных данных”	обозначает нарушение безопасности, в результате которого происходит случайное или незаконное уничтожение, потеря, изменение, несанкционированное раскрытие или доступ к передаваемым, хранящимся или обрабатываемым Персональным данным.
“Согласие субъекта данных”	обозначает любое предоставленное свободно, конкретное, информированное и недвусмысленное свидетельство о намерениях

	субъекта Данных, согласно которому он своим конкретным заявлением или явным одобряющим действием демонстрирует свое согласие на обработку персональных данных.
“Ответственный за защиту данных по странам ЕС”	обозначает работника Группы, отвечающего за реализацию Политики в части Группы, действующей на территории ЕС
“Глобальный Ответственный за защиту данных”	обозначает работника Группы, отвечающего за реализацию Политики в рамках Группы
“Локальный Ответственный за защиту данных”	обозначает работника участника Группы, отвечающего за реализацию Политики в рамках участника Группы
“Договор с Центром обработки данных”	обозначает договор, заключенный между участником Группы и любым контрагентом в отношении реализации Политики в рамках соответствующего участника Группы
“График хранения”	обозначает специальный график, в соответствии с которым документы хранятся в течение конкретного периода времени.

2. Применение

2.1. Предназначение

В настоящей Политике излагаются ключевые принципы Защиты Персональных данных и Обработки Персональных данных, применимые к Группе.

В качестве работодателя, клиента и поставщика каждый участник Группы осуществляет сбор и использует персональные данные работников, деловых партнеров, клиентов, потенциальных клиентов и т.п. Хотя работа с такими персональными данными является необходимым условием осуществления нашей деятельности, Группа понимает, что защита личных прав и неприкосновенности частной жизни каждого человека составляет основу доверия во всех отношениях. Именно по этой причине Группа намерена организовать наиболее оптимальным образом защиту и Обработку Персональных данных.

Для Группы крайне важно выполнять требования к Защите Персональных данных в странах осуществления ее хозяйственной деятельности и проживания субъектов Данных. Все участники Группы обязаны выполнять местные требования, предъявляемые во всех странах мира к контролю и обработке персональных данных.

Важнейшим приоритетом Группы является обеспечение универсальной применимости и выполнения во всемирном масштабе стандартов обработки персональных данных. Настоящая Политика Защиты Данных представляет собой общие рамки, применимые ко всем подразделениям Группы. С учетом различия местных нормативно-правовых актов и разнообразия деятельности участников Группы, в то же время неизбежно, что реализация настоящих принципов Защиты Данных может несколько различаться для тех или иных участников Группы.

С настоящей Политикой должны быть ознакомлены все работники, которые обязаны соблюдать положения Политики и выполнять ее требования. Кроме того, Политика применима к контрагентам, а также лицам, совершающим сделки с Группой и имеющим или способным получить доступ к Персональным данным. Такие контрагенты должны ознакомиться, уяснить и выполнять положения настоящей Политики.

2.2. Сфера применения и обязательные юридические требования

Страны, в которых осуществляется деятельность Группы, можно разделить на 3 крупных группы в зависимости от местонахождения: ЕС, Россия и другие страны.

За исключением главных офисов, находящихся в Швейцарии и России, некоторые участники Группы находятся на территории ЕС. Правила защиты данных, действующие в ЕС (Положение (ЕС) 2016/679 ("Общее положение о защите данных" или "GDPR"), являются строгими и применяются на гармонизированной основе на всей территории ЕС. Сфера применения GDPR выходит за пределы ЕС, поскольку это положение применимо также к участникам Группы, учрежденным за пределами ЕС, если субъект Данных является резидентом ЕС.

Группа обязалась руководствоваться принципами и обязательствами, предусмотренными GDPR, в качестве основы своей Политики защиты Данных. В то же время отдельные участники Группы обязаны также выполнять требования местных нормативно-правовых актов. Настоящая Политика защиты Данных является лишь дополнением к местным нормативно-правовым актам,

регулирующим Защиту Данных. Соответствующие местные нормативно-правовые акты имеют преимущественную силу в случае, если они противоречат настоящей Политике защиты Данных или содержат более строгие требования, по сравнению с настоящей Политикой защиты Данных. Примерами местных нормативно-правовых актов, которыми должны руководствоваться некоторые участники Группы, являются:

- Федеральный закон № 152-ФЗ "О персональных данных" 2006 года (применим к России);
- Федеральный закон о защите данных (FADP) от 19 июня 1992 года (применим к Швейцарии);
- Местное законодательство, регулирующее вопросы корпоративного управления и периоды сохранения данных.

3. Общие положения

3.1. Цели Политики

Основными целями Политики являются:

- Защита прав и свобод всех субъектов Данных и их информирование об этом;
- Соблюдение правил обработки Персональных данных;
- Предотвращение любых нарушений обработки Персональных данных и проблем с безопасностью в целом;
- Повышение осведомленности о режиме защиты Персональных данных в целом.

3.2. Принципы Политики

Вся обработка Персональных данных должна осуществляться в соответствии с принципами Защиты Данных, указанными в GDPR. Политика и процедуры Группы призваны обеспечить соблюдение указанных принципов.

Вкратце, мы как Группа обязуемся выполнять следующие принципы:

- Принцип объективности и законности: мы обязуемся обрабатывать персональные данные лишь при условии, что субъект данных был проинформирован об этом и имеются правовые основания для обработки.

- Принцип ограничения цели: мы осуществляем обработку персональных данных лишь для достижения четко обозначенных и законных целей и не обрабатываем такие данные в форме, не совместимой с этими целями.

- Принцип минимального объема данных: мы обрабатываем лишь персональные данные, являющиеся достаточными, соответствующими цели и ограниченными объемом, необходимым для целей, которые ставятся при обработке таких данных.

- Принцип точности: мы обрабатываем лишь те данные, которые являются точными и, если необходимо, актуальными. Мы принимаем все разумные меры для того, чтобы обеспечить незамедлительное уничтожение или исправление персональных данных, являющихся неточными.

- Принцип ограничения обработки: мы содержим все персональные данные в форме, позволяющей идентифицировать субъекты Данных в течение периода, не превышающего то время, которое необходимо для целей, в которых осуществляется обработка персональных данных.

- Принцип обеспечения безопасности: мы осуществляем обработку данных лишь в форме, обеспечивающей надлежащую безопасность, включая защиту от несанкционированной или незаконной обработки и от случайной потери, уничтожения или изменения, с применением всех необходимых мер технического или организационного характера.

- Принцип подотчетности: мы несем ответственность и должны быть способны продемонстрировать в любое время выполнение вышеуказанных принципов защиты данных представителям компетентных органов или субъектам данных.

4. Меры по защите данных

Готовность Группы реализовать на практике указанные выше принципы Защиты Данных подтверждают следующие принятые нами меры:

4.1. Законность и объективность обработки

Группа обеспечивает объективность и законность сбора и обработки данных. Мы принимаем все разумные меры для того, чтобы персональные данные были актуальными, точными и хранились лишь в течение заранее установленного периода времени.

Группа обеспечивает, чтобы, в зависимости от категории, к которой относится субъект Данных, собранные данные использовались лишь на основе указанных выше принципов объективности и законности.

4.1.1. Данные работников

Под данными работников понимаются все данные, обрабатываемые любым участником Группы, которые относятся к работникам и (при необходимости) их супругам. В то же время понятие "данные работников" шире, чем просто персональные данные действующих работников. Существуют и другие категории данных, относящихся к работе по найму, например, данные работников, вышедших на пенсию, и лиц, подавших заявления о приеме на работу.

Сбор данных всех работников осуществляется участником Группоы, где работал работник. Работодатель выступает в качестве Контролера данных (это означает, что Группа определяет цели и средства обработки данных).

1. Правовые основания для деятельности по обработке

В отношениям между работодателем и работником подавляющая часть деятельности по обработке данных юридически обоснована необходимостью выполнения договора: участники Группы не могли бы надлежащим образом выполнить свои обязательства по своим трудовым договорам, если бы они были лишены возможности обрабатывать данные своих работников.

Юридическим основанием некоторой деятельности по обработке данных является юридическое обязательство: во всех странах, в которых участники Группы осуществляют свою хозяйственную деятельность, существует юридическое обязательство обрабатывать определенные персональные данные работников, например, для целей социальной защиты, страхования, выплаты должностных окладов и т.п.

Кроме того, некоторая деятельность по обработке данных может быть разрешена коллективными договорами. Коллективные договоры содержат договоренность (договоренности) о размере оплаты труда между работодателями и представителями работников в объемах, разрешенных соответствующим трудовым законодательством. В договорах должна быть предусмотрена конкретная цель предполагаемой деятельности по обработке данных с обязательным учетом параметров национального законодательства о защите данных.

Каждый участник Группы почти во всех случаях может также полагаться на законные интересы обработки персональных данных, исходя из потребностей надлежащего функционирования предприятия (например, когда участник Группы не имеет трудового договора с претендентами на занятие должностей, но Группа на законных основаниях заинтересована в оценке потенциальных кандидатов, в частности, когда они подают участникам Группы заявления о приеме на работу).

В весьма ограниченном количестве случаев деятельность по обработке может быть обоснована прямым согласием, предоставленным работником (например, при публикации интервью или фотографии во внутреннем издании и т.п.).

Каждый участник Группы несет исключительную ответственность за определение законности оснований для деятельности по обработке данных.

2. Объективность обработки

Детальные сведения о том, как обрабатываются данные работников, можно найти в наших более детальных политиках. В настоящем документе содержится краткий обзор некоторых аспектов деятельности по обработке:

- Минимальный объем: Группа обеспечивает ограничение обрабатываемых данных работников минимально необходимым объемом.
- Точность: Группа обеспечивает регулярную актуализацию данных всех работников на уровне организации и возможность для каждого работника в любое время потребовать исправления любых неправильных данных.
- Ограничение периода хранения: данные всех работников обрабатываются в течение срока действия трудового договора. После прекращения действия трудового договора большая часть данных уничтожается, с учетом установленного периода их сохранения, если иное не предусмотрено законом или субъект данных не предоставил свое недвусмысленное

согласие на сохранение своих данных в деле для дальнейшей конкретной деятельности по обработке.

- Безопасность: Все персональные данные обрабатываются в безопасной форме. Например, доступ к данным ограничивается служебной необходимостью, данные Группы часто обезличиваются при их передаче третьим сторонам и т.п.
- Обработка данных ограниченного доступа: такие данные, например, отражающие расовое или этническое происхождение, политические взгляды, религиозные или философские воззрения, членство в профсоюзных организациях, состояние здоровья и особенности частной жизни субъекта данных, обрабатываются с применением необходимых дополнительных мер предосторожности.
- Группа сводит к минимуму объемы автоматизированной обработки персональных данных. В том случае, если персональные данные обрабатываются автоматически в рамках трудовых отношений, и производится оценка конкретных персональных сведений (например, в рамках подбора персонала или оценки навыков), такая автоматизированная обработка не может быть исключительной основой для принятия решения, которое может иметь отрицательные последствия или создать значительные проблемы для соответствующего работника.

Каждый участник Группы несет исключительную ответственность за объективность обработки данных работников.

4.1.2. Данные контрагентов

Под данными контрагентов понимаются персональные данные клиентов, субподрядчиков, поставщиков, деловых партнеров, посетителей вэб-сайта и т.п. Хотя эти данные всегда представляют собой профессиональный данные, т.е. обработка данных ограниченного доступа в таких случаях не осуществляется, каждый адрес электронной почты или телефонный номер рассматривается в качестве персональных данных.

Насколько Группа осуществляет сбор данных контрагентов непосредственно у субъекта данных, она выступает в качестве Контролера Данных. Характер деятельности Группы может потребовать сбора данных контрагентов у другой стороны. В таком случае Группа выступает лишь в качестве Центра обработки данных, а не Контролера данных, если не достигнута иная договоренность.

1. Правовые основания для деятельности по обработке

В рамках договорных отношений обработка данных в подавляющем большинстве случаев юридически обоснована необходимостью выполнения договора: Группа не могла бы надлежащим образом выполнить обязательства по своим договорам, если бы она была лишена возможности обрабатывать соответствующие данные.

Некоторая деятельность по обработке данных обоснована необходимостью выполнения юридического обязательства: в ряде стран, в которых Группа осуществляет свою деятельность, существует юридическая обязанность обработки поставщиками некоторых персональных данных.

Группа практически во всех случаях может полагаться на законную заинтересованность в обработке персональных данных, поскольку это необходимо для обеспечения надлежащего функционирования предприятия.

В весьма немногих случаях может потребоваться обоснование необходимости деятельности по обработке прямым согласием, предоставленным третьей стороной (например, получение информационной рассылки Группы и т.п.).

Насколько данные Контрагентов контролируются Группой (это означает, что участник Группы определяет цели и средства обработки данных), Группа отвечает за правовое обоснование деятельности по обработке.

2. Объективность обработки

Детальные сведения о том, как обрабатываются данные контрагентов, можно найти в наших более детальных политиках. В общем плане, применяются определенные принципы, применимые к обработке данных работников, о чем говорится в пункте 4.1.1.

Необходимо отметить следующие дополнительные принципы:

- В случае обработки сбор данных контрагентов осуществляется через вэб-сайт Группы и онлайн-инструменты: в том случае, если сбор, обработка и использование персональных данных осуществляются на вэб-сайте, субъекты данных должны быть проинформированы об этом в форме заявления о защите неприкосновенности частной жизни и, в применимых случаях, информации об идентификационных файлах. Заявление о защите неприкосновенности частной жизни и любая информация об идентификационных файлах должны быть объединены таким образом, чтобы субъекты данных могли легко найти их с возможностью прямого и непротиворечивого доступа.

  Насколько мы создаем на наших вэб-сайтах профили пользователей (ведем учет), субъекты данных всегда должны быть проинформированы об этом в заявлении о защите неприкосновенности частной жизни. Персональный учет может осуществляться лишь в том случае, если это разрешено национальным законодательством, или с согласия субъекта Данных.

  В том случае, если доступ с вэб-сайта или из приложения к персональным данным в той или иной области ограничивается кругом зарегистрированных пользователей, идентификация и отождествление субъекта Данных обеспечивает дополнительную защиту доступа.

- Цифровой маркетинг: Группа осуществляет цифровой маркетинг лишь в ограниченном контексте отношений меду конкретными предприятиями при отсутствии юридического требования получения согласия на осуществление цифрового маркетинга для физических лиц при условии, что им должна быть предоставлена возможность выйти из программы по своему усмотрению.

  В то же время Группы, как правило, всегда стремится получить согласие до рассылки рекламных материалов или осуществления прямого маркетинга в отношении того или иного субъекта Данных контрагента.

Насколько Группа выступает в качестве Контролера данных контрагентов, Группа отвечает за определение правовых оснований для деятельности по обработке данных.

4.1.3.Согласие

Насколько Группа полагается на согласие в качестве правового основания для обработки, применяются следующие условия:

Заявления о согласии должны делаться добровольно, в письменном виде и в соответствии с местными нормативно-правовыми требованиями. Любое согласие, не отвечающее этим условиям, не имеет юридической силы. Заявление о согласии должно быть предоставлено в письменном виде или в электронной форме с документальным оформлением. До предоставления согласия субъект Данных информируется об объеме деятельности по обработке. Субъект Данных вправе отозвать свое согласие в любое время.

В отношении данных ограниченного доступа должно быть получено прямое письменное согласие от субъекта Данных, если четкие альтернативные правовые основания для такой обработки отсутствуют.

В большинстве случаев согласие на обработку Персональных и данных ограниченного доступа получается Группой в установленном порядке на основе стандартных документов о предоставлении согласия.

4.2. Защита прав субъектов данных

Каждый участник Группы должен обеспечить, чтобы субъект данных, Персональные данные которого обрабатываются Группой, имел возможность воспользоваться следующими индивидуальными правами.

- **Право на получение информации:**

  Политика содержит подробный обзор общих принципов, которыми руководствуется Группа при обработке Персональных данных. О них должны быть проинформированы субъекты данных при сборе их Персональных данных (насколько Группа выступает в качестве Контролера) и они публикуются на вэб-сайте www.eurochemgroup.ru.

  В то же время, если того недвусмысленно требует субъект данных, соответствующий участник Группы (т.е. Контролер или Центр обработки Персональных данных) должен предоставить субъекту данных информацию о его обработанных Персональных данных в краткой, прозрачной, ясной и легко доступной форме. Кроме того, участник Группы оставляет за собой право отклонить просьбу о предоставлении информации, если субъект данных уже имеет информацию или это может потребовать непропорционально больших усилий.

  По соответствующему требованию участник Группы должен предоставить следующую информацию: 1) название и контактные реквизиты организации, 2) цели обработки, 3) правовые основания для обработки; 4) категории полученных Персональных данных; 5) получатели или категории получателей персональных данных, 6) сведения о передаче Персональных данных в любые третьи страны или международные организации (в применимых случаях), 7) периоды сохранения персональных данных, 8) права, предоставляемые субъектам данных в связи с обработкой, 9) право отозвать согласие (в применимых случаях), 10) право направить жалобу в надзорный орган.

- **Право доступа:**

В целях обеспечения осведомленности субъектов данных о законности деятельности по обработке и ее проверки Группа предоставляет им право на получение подтверждения того, что данные субъекта данных обрабатываются; доступ к персональным данным; и необходимую дополнительную информацию. Форма доступа подлежит взаимному согласованию.

- **Право на исправление:**

  В том случае, если участник Группы обрабатывает неточные или неполные персональные данные, субъект данных вправе потребовать исправления или дополнения данных. В этой связи участник Группы оставляет за собой право отказать в просьбе об исправлении, если это разрешено применимым положением.

- **Право на удаление и право на ограничение обработки:**

  Субъекты данных вправе удалить свои Персональные данные из документации Группы, если 1) в Персональных данных отсутствует дальнейшая необходимость для целей, в которых они первоначально собирались или обрабатывались; 2) участник Группы полагался исключительно на согласие в качестве правового основания для хранения данных, и субъект данных отозвал свое согласие; 3) участник Группы полагается исключительно на законные интересы в качестве основания для обработки, и субъект данных возражает против обработки своих данных при отсутствии приоритетного законного интереса, который мог бы обосновать продолжение такой обработки; 4) участник Группы обрабатывает Персональные данные для целей прямого маркетинга; 5) участник Группы обрабатывал Персональные данные незаконно.

  В качестве альтернативы требованию об удалении персональных данных субъект данных вправе потребовать от Участника Группы ограничить обработку своих Персональных данных хранением данных, но не использовать их иным образом. Такое ограничение может быть запрошено в следующих случаях: 1) субъект данных оспаривает точность своих Персональных данных и участник Группы при этом проверяет точность данных; 2) данные обрабатывались незаконно, но субъект данных выступает против их удаления и требует лишь ограничения их обработки; 3) участник Группы более не нуждается в Персональных данных, но субъекту данных необходимо сохранять Персональные данные для целей обоснования, возбуждения или защиты от судебного иска; 4) субъект данных возражает против обработки данных участником Группы, но участник при этом ищет законные основания, которые имели бы преимущественную силу по отношению к доводам, которые приводятся субъектом данных.

- **Право на обеспечение переносимости данных:**

  В строго определенных условиях субъект данных вправе потребовать от участника Группы предоставить ему все его Персональные данные в структурированной, обычно

используемой и машиночитаемой форме. Это должно предоставить субъекту данных возможность передать свои данные в другую организацию. При наличии такой технической возможности субъект данных вправе потребовать передачи данных непосредственно в эту другую организацию.

Право на обеспечение переносимости данных применяется лишь: 1) в отношении Персональных данных, предоставленных физическим лицом тому или иному Контролеру; 2) в случае, когда обработка производится с согласия субъекта данных или для целей выполнения договора; и 3) если обработка производится с помощью автоматических средств.

- **Право на выдвижение возражений:**

  В том случае, если субъект данных возражает против обработки своих Персональных данных на “основаниях, касающихся его конкретных обстоятельств”, субъект данных вправе возразить против: 1) обработки, исходя из своих законных интересов, и 2) прямого маркетинга (включая указание на биографические данные).

  В этом случае участник Группы обязан прекратить обработку Персональных данных, если: 1) он не сможет продемонстрировать наличие других законных оснований, обосновывающих право на обработку и имеющих преимущественную силу по сравнению с интересами, правами и свободами субъекта данных; или 2) обработка не осуществляется для целей обоснования, возбуждения или защиты от судебных исков.

Все требования об использовании указанных выше прав должны направляться Ответственному за защиту данных. Если применимым нормативно-правовым актом не разрешено иное, каждое требование должно быть оформлено в письменном виде.

Если тем или иным применимым нормативно-правовым актом не предусмотрено иное, ответ на каждое требование должен быть направлен не позднее 30 дней после получения письменного требования от субъекта данных. Соответствующая проверка должна подтвердить, что лицо, обратившееся с требованием, является субъектом данных или его уполномоченным законным представителем.

Если тем или иным применимым нормативно-правовым актом не предусмотрено иное, каждое требование выполняется бесплатно, если оно не будет сочтено необоснованным или излишним по своему характеру.

4.3. Безопасность Персональных данных

Группа обязуется выполнять требования передовой практики отрасли в отношении безопасности информационных технологий.

Кроме того, каждая Компания Группы приняла физические, технические и организационные меры по обеспечению безопасности персональных данных. Это включает предотвращение потери или повреждения, несанкционированного изменения, доступа или обработки и иных рисков, которым

они могут быть подвержены в результате действий персонала, физического воздействия или воздействия внешних условий.

Хотя меры защиты различаются в зависимости от конкретного участника Группы, следующие меры считаются минимально необходимыми:

Все Персональные данные должны рассматриваться в качестве данных, требующих применения максимально строгих средств защиты и должны содержаться:

- в запираемом помещении с контролируемым доступом; и/или
- в запираемом шкафу или сейфе для хранения документов; и/или
- в случае, если они представлены в компьютеризированной форме, должны быть защищены паролем в соответствии с корпоративными требованиями; и/или
- должны храниться на (съемном) компьютерном носителе информации в зашифрованном виде.

Документация в бумажном виде не должна оставляться в местах, в которых она может попасть в руки персонала, не имеющего разрешения на ее использование, и не должна выноситься из хозяйственных помещений без специального разрешения. После того, как дальнейшая потребность в бумажной документации для повседневной поддержки клиентов отпадет, она должна быть удалена из архива.

Персональные данные могут быть удалены или уничтожены лишь в соответствии с Графиком хранения.

Группа должна обеспечить, чтобы Персональные данные не раскрывались лицам, не имеющим соответствующего разрешения, включая членов семьи, друзей, государственные органы, если законом не предусмотрено иное. Все требования о предоставлении данных по одной из этих причин должны быть подтверждены соответствующими документами, и любое раскрытие информации такого рода должно быть специально разрешено Ответственным за защиту данных.

Каждый участник Группы должен обеспечить, чтобы все работники соблюдали требования настоящей Политики и Кодекса поведения. Кроме того, каждый участник Группы гарантирует, что все работники, отвечающие за реализацию Политики, будут иметь надлежащий уровень подготовки, информирования и поддержки (см. также статью 4.6)

4.4. Нарушение обработки Персональных данных

Под нарушением обработки Персональных данных понимается нарушение безопасности, ведущее к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к Персональным данным, переданным, хранящимся или обрабатываемым иным образом. Это может иметь форму инцидента технического или физического характера. С учетом того, что нарушение обработки всегда является полным сюрпризом, каждый участник Группы принял все разумные меры для предотвращения того, чтобы нарушение обработки персональных данных не привело к катастрофе.

Каждый участник Группы имеет надежные процедуры выявления, расследования и информирования о случаях нарушения обработки. Их описание содержится в Политике Компании Группы в вопросах нарушения защиты Персональных обработки данных. Кроме того, каждый участник Группы ведет реестр нарушений обработки данных, в который заносятся сведения обо всех фактах нарушения обработки Персональных данных, последствиях нарушения обработки, предпринимаемых усилиях и мерах по устранению нарушений.

Хотя политика различных участников может предусматривать разные меры, каждая процедура, применяемая в случае нарушения обработки данных, должна предусматривать принятие следующих мер:

- Все работники должны немедленно информировать своего непосредственного начальника о случаях нарушения настоящей Политики или иных положений о защите персональных данных (инцидентах касательно Защиты Данных). После этого непосредственный начальник должен проинформировать Локального Ответственного за защиту данных, Ответственного за защиту данных по странам ЕС и Глобального Ответственного за защиту данных.

- Ответственные за защиту данных принимают решение о том, приводит ли инцидент нарушения Защиты Данных к фактическому нарушению обработки персональных данных. Например, потеря USB-накопителя, кража портативного компьютера, заражение вирусом или взлом базы данных, содержащей персональные данные, рассматриваются в качестве случаев нарушения обработки персональных данных. Угроза или упущение в системе защиты, например, слабые пароли или устаревшие брандмауэры, не считаются нарушением обработки персональных данных, если не произошла утечка персональных данных.

- В том случае, если инцидент нарушения Защиты Данных действительно привел к нарушению обработки персональных данных, Ответственные за защиту данных должны расследовать объем нарушения обработки. Необходимо расследовать объем нарушения обработки персональных данных, возможное количество пострадавших субъектов Данных, возможность того, что нарушение обработки может привести к нарушению прав и свобод субъектов Данных, содержат ли нарушенные персональные данные ограниченного доступа, были ли нарушенные данные защищены (зашифрованы и т.п.), вовлечены ли в нарушение обработки данных другие стороны и меры, которые следует принять для предотвращения (дальнейшей) потери Персональных данных.

- На основании указанной оценки Ответственные за защиту данных должны принять решение относительно необходимости проинформировать соответствующий надзорный орган, и Субъект Данных должен быть проинформирован о нарушении обработки. В уведомлении надзорного органа нет необходимости, если нарушение обработки Персональных данных едва ли угрожает индивидуальным правам и свободам.

- В том случае, если требуется уведомление о нарушении обработки персональных данных, Группа уведомляет компетентный надзорный орган и предоставляет ему всю необходимую информацию в течение 72 часов после того, как ей станет известно о таком нарушении.

- В том случае, если нарушение обработки персональных данных сопряжено с ''высоким риском'' для индивидуальных прав и свобод, Группа должна немедленно уведомить соответствующих лиц. Под ''высоким риском'' понимается ситуация, когда порог уведомления физических лиц выше порога уведомления соответствующего надзорного органа. В том случае, если уведомление физических лиц требует несоразмерных усилий, Группа может использовать ту или иную форму публичного информирования при условии, что эта форма позволит проинформировать в равной мере всех заинтересованных лиц.

- Для обеспечения высокого уровня наглядности и прозрачности каждый участник Группы обязан отразить документально все инциденты нарушения Защиты Данных (независимо от информирования о них), включая факты, относящиеся к нарушению, его последствия и принятые или планируемые меры. Вся указанная документация требуется Надзорному органу для целей подтверждения выполнения требований уведомления. Все факты, касающиеся нарушения обработки данных, должны быть обобщены в специальной форме “Реестр нарушений обработки данных” (Приложение 2).

4.5. Хранение и уничтожение данных

Как отмечалось выше в статье 4.1 настоящей Политики, обработка Персональных данных не должна осуществляться дольше, чем это необходимо для целей такой обработки.

Каждый участник Группы имеет собственный График хранения в соответствии с Приложением 3. Сроки хранения определяются с учетом требований местного законодательства к различным категориям Персональных данных. Обычно местным законодательством устанавливаются следующие категории персональных данных:

1. Бухгалтерский учет и финансы
2. Договоры
3. Корпоративная документация
4. Переписка и внутренние информационные материалы
5. Электронная почта и иная электронная корреспонденция
6. Юридические дела и документация
7. Документация по вопросам заработной платы
8. Документация по вопросам пенсий
9. Документация по кадровым вопросам
10. Документация по налоговым вопросам

В любом случае все персональные данные должны храниться в течение минимального периода, позволяющего Группе возбуждать иски или осуществлять защиту в суде в соответствии с требованиями местного законодательства.

4.6. Обучение персонала

Группа обеспечивает, чтобы все работники, имеющие доступ к Персональным данным, прошли вводную подготовку по вопросам выполнения своих обязанностей, предусмотренных настоящей Политикой. Кроме того, каждый участник Группы должен обеспечить регулярноеобучение своих

работников по вопросам Защиты Данных и предоставлять им рекомендации по процедурным вопросам.

Локальный Ответственный за защиту данных отвечает за организацию необходимого обучения всех Работников. Формы такого обучения могут различаться в зависимости от целевой аудитории, количества работников, проходящих обучение, целей обучения и иных обстоятельств.

Обучение должно осуществляться на регулярной основе. Каждый участник Группы устанавливает собственные конкретные сроки в соответствии с требованиями и с учетом предложений Глобального Ответственного за защиту данных или Ответственного за защиту данных по странам ЕС.

4.7. Документация, связанная с деятельностью по обработке

Каждая Компания Группы имеет реестр, отражающий все Персональные данные, которые она обрабатывает и контролирует, и вносит их в реестр данных (Приложение 4).

Указанный реестр данных обеспечивает выполнение Компаниями Группы ряда важнейших требований, касающихся подотчетности, согласно GDPR:

- Ведение учета всей деятельности по обработке;
- Ведение учета договоров с центрами обработки данных;
- Ведение учета нарушений обработки данных, включая уведомления о нарушениях, направляемые надзорным органам и субъектам данных.

Хотя содержание реестров данных различных участников Группы может различаться, реестр должен содержать по меньшей мере следующие сведения о деятельности по обработке:

- наименование и контактные реквизиты Группы и, в применимых случаях, Контролера (Контролеров) и его (их) представителя (представителей);
- цели деятельности по обработке;
- описание категорий субъектов данных и категорий персональных данных;
- категории получателей, которым Персональные данные были или будут раскрыты, включая получателей их третьих стран или международных организаций;
- в применимых случаях - передача Персональных данных в третью страну или международной организации, включая идентификационные сведения о такой третьей стране или международной организации;
- по возможности - предполагаемые сроки уничтожения различных категорий данных;
- по возможности - общее описание технических и организационных мер защиты, принятых Группой.

Каждый участник Группы несет исключительную ответственность за ведение реестра.

4.8. Передача данных

В целях компенсации возможного отсутствия Защиты данных при передаче Персональных данных третьим сторонам принимаются дополнительные меры безопасности. Группа идентифицировала три типовых случая передачи данных внутри организации, каждый из которых сопровождается принятием различных мер защиты:

- внутригрупповая передача данных: в целях оптимизации передачи данных должны быть реализованы Обязательные корпоративные правила. Эти правила, одобренные надзорным органом, являются юридически обязательными для всех Участников Группы. Среди прочего эти Обязательные корпоративные правила указывают цели передачи и затрагиваемые категории данных; отражают требования GDPR; подтверждают, что экспортеры данных, находящиеся в ЕС, принимают ответственность от имени всей группы; поясняют порядок подачи жалоб; и устанавливают механизмы обеспечения выполнения требований (например, проведение аудита).

- передача данных контрагентам, находящимся внутри Европейской экономической зоны (или в одной из других стран, которые считаются предоставляющими аналогичный уровень защиты), которые выступают в качестве Центра обработки данных: в этих случаях передача данных осуществляется в соответствии с GDPR.

  До передачи любых данных третьей стороне каждый участник Группы применяет процедуры предварительной проверки и оценивает выполнение контрагентом применимых требований.

  После указанной оценки участник Группы должен заключить договор с каждым из таких сторонних Центров обработки данных (договор со сторонним Центром обработки данных). Все такие договоры содержат по меньшей мере следующую информацию:

- передача данных организации, не являющейся участником Группы и находящейся за пределами Европейской экономической зоны, насколько применимо GDPR (когда участник Группы находится в ЕС или субъект данных является резидентом ЕС):

  В дополнение к заключению указанного договора с центром обработки данных каждый участник Группы должен убедиться, что контрагент, которому направляются Персональные данные, применяет достаточные дополнительные меры защиты. Если такие меры не принимаются, участник Группы не передает информацию такой третьей стороне.

4.9. Оценка эффекта защиты данных

Для обеспечения того, чтобы все требования Защиты Данных автоматически определялись и учитывались при проектировании новых систем или процессов и/или анализе работы либо расширении существующих систем или процессов, каждый участник Группы должен обеспечить проведение Оценки эффекта защиты данных (DPIA) в отношении всех новых и/или измененных систем или процессов, за которые он отвечает.

Указанная оценка DPIA проводится совместно с Глобальным Ответственным за защиту данных и Ответственным за защиту данных по странам ЕС. В применимых случаях Департамент информационных технологий (IT) в рамках своей системы информационных технологий и процесса анализа проекта приложения должен сотрудничать с Ответственным за защиту данных в оценке влияния любой новой технологии на безопасность персональных данных.

4.10. Ответственные за защиту данных

4.10.1. Ответственные за защиту данных

Поскольку Группа действует в разных юрисдикциях, включая ЕС, назначаются различные Ответственные за защиту данных:

- Глобальный Ответственный за защиту данных (отвечает за Группу в целом):

  Глобальный Ответственный за защиту данных назначается и освобождается от должности Главным исполнительным директором по согласованию с Главным юридическим советником и Главным финансовым директором.

  Глобальным Ответственным за защиту данных Группы является Александр Пузанов. Его контактные данные: Aleksander.Puzanov@eurochem.ru

- Ответственный за защиту данных по странам ЕС (отвечает за деятельность Группы в странах ЕС):

  Ответственный за защиту данных по странам ЕС назначается и освобождается от должности Главным исполнительным директором по согласованию с Глобальным Ответственным за защиту данных.

  Ответственным за защиту данных по странам ЕС Группы является Pieter Callens. Его контактные данные: Pieter.Callens@eurochem.be.

- Локальные Ответственные за защиту данных (в случае его назначения отвечает за деятельность того или иного участника Группы):

  Каждый участник Группы вправе назначить Локального Ответственного за защиту данных. Локальный Ответственный за защиту данных назначается и освобождается от должности Главным исполнительным директором (генеральным менеджером) участника Группы. В том случае, если Локальный Ответственный за защиту данных не назначается, функции Локального Ответственного за защиту данных выполняются Главным исполнительным директором (генеральным менеджером).

4.10.2. Обязанности Ответственных за защиту данных

Глобальный Ответственный за защиту данных

Глобальный Ответственный за защиту данных назначается с учетом его профессиональных качеств, и в частности экспертных знаний в области законодательства и практики защиты персональных данных и способности выполнять следующие обязанности Глобального Ответственного за защиту данных:

- предоставление руководству Группы рекомендаций по вопросам Политики и оказание ему помощи в связи со значительными угрозами, факторами, вызывающими озабоченность, и проблемами в сфере Защиты Данных в случае их возникновения;
- создание и обеспечение функционирования высококачественной Системы Защиты данных в рамках Группы;
- управление стратегией и инициативами в области связи, обучения или профессиональной подготовки и обеспечение поддержки Хозяйственных подразделений в вопросах Защиты данных, если это необходимо;
- контроль деятельности Ответственного за защиту данных по странам ЕС и Локальных Ответственных за защиту данных (в случае их назначения).

В сотрудничестве с Ответственным за защиту данных по странам ЕС и Локальными Ответственными за защиту данных (в случае их назначения):

- обеспечение наличия соответствующих процедур и политик в Группе для сохранения точности и актуальности Персональных данных, с учетом объема собранных данных, скорости их возможного изменения и любых других соответствующих факторов;
- осуществление регулярной подготовки персонала по вопросам Защиты данных, предоставление пояснений по соответствующим вопросам и проблемам;
- информирование и предоставление рекомендаций Группе и работникам, осуществляющим обработку, в отношении их обязанностей, установленных в соответствии с настоящей Политикой;
- мониторинг выполнения требований настоящей Политики и проведение аудита;
- предоставление, по соответствующей запросу, рекомендаций по вопросам оценки последствий для Защиты данных и мониторинга ее эффективности;
- мониторинг и анализ изменений, вносимых в применимое законодательство;
- анализ сроков хранения всех Персональных данных, обрабатываемых Группой, и выявление любых данных, дальнейшая потребность в которых для заявленной цели отсутствует;
- принятие соответствующих мер в случаях, когда контрагенту могут быть переданы неточные или неактуальные персональные данные, информирование их о том, что информация является неточной и/или неактуальной и не должна использоваться в качестве основы для принятия решений относительно соответствующих лиц; и внесение любых исправлений в Персональные данные, предоставляемые контрагенту, если это необходимо;
- анализ размера возможного ущерба или убытков, которые могут быть нанесены физическим лицам (например, работникам или контрагенту) в случае нарушения

безопасности, воздействия любого нарушения безопасности на саму Группу и любого возможного репутационного ущерба, включая возможную потерю доверия клиентов.

Ответственный за защиту данных по странам ЕС

Ответственный за защиту данных по странам ЕС должен быть резидентом ЕС и должен назначаться на основе профессиональных качеств, в частности экспертных знаний в области законодательства и практики Защиты данных и способности выполнять следующие обязанности в дополнение к указанным выше обязанностям:

- сотрудничество с надзорными органами ЕС, Глобальным Ответственным за защиту данных и Локальными Ответственными за защиту данных (в случае их назначения);
- выполнение функций представителя для контактов с надзорными органами по вопросам обработки и нарушения обработки данных;
- мониторинг и анализ изменений, вносимых в законодательство ЕС, и предоставление Глобальному Ответственному за защиту данных информации о таких изменениях.

Локальный Ответственный за защиту данных

Каждый участник Группы вправе назначить Локального Ответственного за защиту данных для оказания помощи Глобальному Ответственному за защиту данных и Ответственному за защиту данных по странам ЕС при выполнении их указанных выше обязанностей.

5. Управление Политикой

5.1. Ответственность

Каждый участник Группы несет исключительную ответственность за выполнение требований настоящей Политики, своих юридических обязательств и надлежащую обработку персональных данных. Выполнение требований Политики является обязательным для работников, связанных с данными процессами.

В случаях, когда существуют основания полагать, что юридические обязательства противоречат обязанностям, предусмотренным настоящей Политикой защиты данных, участник Группы обязан проинформировать об этом Глобального Ответственного за защиту данных. В случае обнаружения противоречий между национальным законодательством и Политикой Группа должна работать совместно с соответствующим участником Группы в поиске практического решения, соответствующего целям Политики защиты Данных.

При наличии соответствующей возможности участник Группы вправе принимать положения, дополняющие или отклоняющиеся от положений настоящей Политики. Такие положения требуют одобрения Глобальным Ответственным за защиту данных Группы.

5.2. Средства контроля

Каждый участник Группы гарантирует, что выполнение требований Политики или информирование о любых совершенных или потенциальных нарушениях не приведет к любым негативным последствиям для работника, предоставившего такую информацию. В то же время Группа должна осуждать любые действия работников, совершенные в нарушение требований Политики.

Группа исходит из того, что должен существовать "Система сообщения о нарушениях и несоответствиях", и предполагает, что работники будут сообщать по такому каналу о любых случаях нарушения или потенциального нарушения Политики. Сведения о таком канале связи должны быть доступны для всеобщего ознакомления и размещаются на корпоративном портале.

Группа оставляет за собой право периодически проверять знания работников по вопросам защиты персональных данных, контролировать выполнение и соблюдение требований настоящей Политики и анализировать ее эффективность.

5.3. Конфиденциальность

Как указано в статье 4.4, на Персональные данные распространяются обязательства по сохранению конфиденциальности.

В том случае, если в некоторых обстоятельствах разрешается предоставление персональных данных без знания или согласия со стороны Субъекта Данных. Это положение применяется в случаях, когда раскрытие Персональных данных необходимо по любой из следующих причин:

• предотвращение или выявление преступления.

• задержание или преследование правонарушителей.

• исчисление или сбор налога или сбора.

• по постановлению суда или в соответствии с любой нормой закона.

В том случае, если любой участник Группы обрабатывает персональные данные для любых из этих целей, он вправе воспользоваться исключением из своего обязательства сохранять конфиденциальность, но лишь в той степени, в которой невыполнение этого положения может нанести ущерб в рассмотрении соответствующего вопроса.

В том случае, если любой участник Группы получает требование суда или любого правоохранительного органа о предоставлении информации в отношении того или иного субъекта Данных, организация обязана немедленно уведомить об этом Глобального Ответственного за защиту данных, который должен предоставить необходимые рекомендации и оказать всестороннее содействие.

5.4. Пересмотр Политики

Настоящая Политика пересматривается Глобальным Ответственным за защиту данных на регулярной основе, но не реже одного раза в год, с целью обеспечения сохранения актуальности Политики и ее соответствия всем применимым правилам и требованиям законодательства.

О любых изменениях должна быть немедленно проинформирована Группа, которая реализует такие изменения.

С последней версией Политики защиты данных можно ознакомиться на вэб-сайте Группы: www.eurochemgroup.com

5.5. Жалобы и вопросы

Все вопросы, касающиеся настоящей Политики и приложений к ней, могут направляться Глобальному Ответственному за защиту данных или соответствующему Локальному Ответственному за защиту данных.

Субъекты Данных, намеревающиеся направить жалобу по поводу обработки своих персональных данных, должны обращаться в письменном виде к Глобальному Ответственному за защиту данных. Расследование жалобы должно быть проведено по существу в каждом конкретном случае надлежащим образом. Глобальный Ответственный за защиту данных должен информировать субъект Данных о ходе и результате рассмотрения жалобы в разумные сроки.

В том случае, если проблема не может быть решена по договоренности между субъектом Данных и Глобальным Ответственным за защиту данных, субъект Данных вправе, по своему усмотрению, прибегнуть к процедуре посредничества, арбитража, судебному разбирательству или передать жалобу в соответствующий орган по обеспечению защиты данных соответствующей юрисдикции.

.

Приложение 1. Ссылки

№ п/п	Идентификационный номер	Название документа	Примечание
Нормативно-правовой документ			
1		Политика по вопросам обеспечения выполнения нормативных требований (комплаенс) EuroChem Group AG	
2		Кодекс поведения EuroChem Group AG	…
3		Федеральный закон "О защите данных" (FADP)	

Приложение 2. Реестр нарушений обработки данных

№	Участник Группы	Категория персональных данных	Описание	Число пострадавших субъектов данных	Контактные реквизиты субъектов данных	Потенциальные последствия	Принятые (планируемые) меры

Приложение 3. График хранения

№	Участник Группы	Категория персональных данных	Тип регистрации	Период хранения

Приложение 4. Реестр данных

№	Участник Группы*	Категория и описание персональных данных*	Цель обработки*	Категории получателей*	Передача третьей стороне	Сроки удаления	Меры защиты

Знаком * помечены графы, требующие обязательного заполнения.