

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «БАСФ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цели Политики обработки персональных данных

Настоящая Политика обработки персональных данных (далее — «Политика») разработана в целях обеспечения надлежащей защиты персональных данных физических лиц, обрабатываемых Оператором обществом с ограниченной ответственностью «БАСФ» (далее — «Оператор» или «ООО «БАСФ»)), а также для выполнения требований законодательства Российской Федерации в области защиты персональных данных.

Цели Политики включают:

Обеспечение безопасности персональных данных: Политика направлена на защиту персональных данных от несанкционированного доступа, утраты, изменения, раскрытия или уничтожения, а также на предотвращение любых других незаконных действий в отношении персональных данных.

Соответствие требованиям законодательства: Политика разработана в строгом соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных», а также с другими нормативными актами, регулирующими защиту персональных данных.

Установление стандартов обработки данных: Политика определяет стандарты и процедуры, обеспечивающие надлежащее и законное обращение с персональными данными в рамках деятельности Оператора, включая их сбор, хранение, использование, передачу и уничтожение.

Информирование субъектов данных: Политика предоставляет субъектам персональных данных информацию об их правах и обязанностях Оператора в отношении обработки их данных, а также о мерах, принимаемых Оператором для обеспечения безопасности данных.

1.2. Принципы обработки персональных данных

Оператор руководствуется следующими основными принципами при обработке персональных данных:

Законность и справедливость обработки: обработка персональных данных осуществляется на законной и справедливой основе, с соблюдением всех требований законодательства Российской Федерации и международных норм.

Целесообразность и пропорциональность: обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Обрабатываются только те данные, которые необходимы для достижения указанных целей, без избыточности.

Конфиденциальность данных: Оператор обеспечивает конфиденциальность персональных данных и принимает необходимые меры для защиты данных от несанкционированного доступа, изменения или уничтожения.

Обеспечение прав субъектов данных: Оператор уважает и соблюдает права субъектов данных, включая право на доступ к своим данным, их исправление и удаление, ограничение обработки и другие права, предусмотренные законодательством.

Прозрачность обработки: Оператор информирует субъектов персональных данных о целях, способах и условиях обработки их данных, а также о правовых основаниях такой обработки.

1.3. Область применения и субъекты персональных данных

Настоящая Политика распространяется на все операции, связанные с обработкой персональных данных, осуществляемые Оператором. Обработка данных охватывает как автоматизированные, так и неавтоматизированные способы обработки, независимо от того, где и как данные обрабатываются: в электронных системах, на бумажных носителях и другими способами.

1.4. Законодательные и нормативные акты, регулирующие обработку данных

Оператор осуществляет обработку персональных данных в соответствии с требованиями законодательства Российской Федерации и международных стандартов. Основными нормативными актами, регулирующими обработку персональных данных, являются:

Федеральный закон № 152-ФЗ «О персональных данных» — основной закон, регулирующий порядок сбора, хранения, использования и защиты персональных данных в Российской Федерации.

Конституция Российской Федерации — закрепляет право граждан на неприкосновенность частной жизни, личную и семейную тайну.

Трудовой кодекс Российской Федерации (РФ) — регулирует порядок обработки персональных данных работников в рамках трудовых отношений.

Гражданский кодекс Российской Федерации (РФ) — устанавливает общие принципы взаимодействия и обязанности сторон в договорных отношениях, связанных с обработкой персональных данных.

Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» — устанавливает особенности обработки данных, осуществляемой без использования информационных систем.

Кроме того, Оператор также руководствуется внутренними нормативными актами, разработанными в соответствии с требованиями законодательства:

- внутренние документы ООО «БАСФ» в области защиты персональных данных;
- локальные нормативно-правовые акты ООО «БАСФ»;
- Устав ООО «БАСФ»,

а также рекомендациями уполномоченных органов и лучшими международными практиками.

Международные акты, такие как GDPR (Общий регламент по защите данных) — применяются в отношении трансграничной обработки данных и международного взаимодействия.

1.5. Основные понятия и определения

Персональные данные — любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Персональные данные включают, но не ограничиваются: фамилию, имя, отчество, дату и место рождения, контактные данные (телефон, адрес электронной почты), паспортные данные, данные о семейном положении, финансовую информацию, данные о состоянии здоровья, а также другую информацию, позволяющую идентифицировать физическое лицо.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с персональными данными с использованием средств автоматизации или без использования таких средств. Обработка включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

Оператор персональных данных — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и средства обработки персональных данных. В контексте настоящей Политики Оператором является общество с ограниченной ответственностью «БАСФ».

Субъект персональных данных — физическое лицо, к которому относятся обрабатываемые персональные данные и которое может быть прямо или косвенно идентифицировано с помощью этих данных. Субъектами персональных данных являются работники Оператора, кандидаты на замещение вакантных должностей, контрагенты, клиенты, пользователи онлайн-сервисов и другие лица, взаимодействующие с Оператором.

Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или юридическому лицу. Трансграничная передача персональных данных осуществляется с соблюдением требований законодательства Российской Федерации, включая обеспечение достаточного уровня защиты прав субъектов персональных данных.

Безопасность персональных данных — состояние защищенности персональных данных, характеризующееся способностью организационных, технических и правовых мер обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке. Безопасность персональных данных включает защиту от несанкционированного доступа, изменения, уничтожения, копирования, распространения и иных незаконных действий.

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе

персональных данных и (или) уничтожаются материальные носители персональных данных. Уничтожение данных осуществляется после достижения целей их обработки или в случае утраты необходимости в их дальнейшем хранении.

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Конфиденциальность персональных данных — обязательное для соблюдения Оператором или иным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники (например, компьютеров, серверов) для выполнения операций с данными, таких как сбор, хранение, использование, передача и уничтожение данных.

Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств, включая программное обеспечение, сервера, сети передачи данных и другие компоненты.

Несанкционированный доступ (несанкционированные действия) — доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней, что может привести к утечке, изменению, уничтожению или блокированию персональных данных.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц, в том числе в рамках договорных отношений или по запросу уполномоченных органов.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц, включая публикацию данных в открытых источниках или их передачу третьим лицам без надлежащего ограничения доступа.

Сайты BASF - <https://www.agro.basf.ru/ru/> <https://shop.basf.ru/>

1.6. Правовые основания обработки персональных данных

1.6.1 Согласие субъекта данных

Согласие субъекта данных является одним из ключевых правовых оснований для обработки персональных данных. Оператор может обрабатывать персональные данные только в том случае, если субъект данных добровольно дал на это свое согласие, за исключением случаев, когда законодательство предусматривает иные основания для обработки.

Ясность и конкретность: Согласие должно быть получено на конкретные цели обработки, описанные в Политике обработки персональных данных. Оно должно быть оформлено четко, без двусмысленных формулировок, и предварительно объяснено субъекту данных.

Форма согласия: Согласие может быть получено в письменной форме, через электронные средства (например, отметкой в чекбоксе на сайте) или другими законными способами, позволяющими подтвердить факт его предоставления.

Отзыв согласия: Субъект данных имеет право в любой момент отозвать свое согласие на обработку персональных данных, при этом Оператор обязан прекратить обработку данных и уничтожить их, если не имеется иных законных оснований для их сохранения.

Примеры: получение согласия используется для обработки данных пользователей сайтов для целей маркетинга, рассылки новостей, или обработки данных кандидатов при подборе персонала.

1.6.2 Выполнение договорных обязательств

Персональные данные могут обрабатываться, если это необходимо для заключения и выполнения договора, стороной которого является субъект данных. Это включает выполнение обязательств Оператора перед субъектом данных по различным типам договоров, включая трудовые договоры, договоры оказания услуг, поставки и т.д.

Соответствие условиям договора: обработка данных в рамках исполнения договора должна соответствовать его условиям, и объем данных должен быть ограничен теми сведениями, которые необходимы для выполнения договорных обязательств.

Использование данных: персональные данные могут использоваться для таких целей, как расчет и выплата заработной платы, управление командировками, исполнение договоров с контрагентами, и другие действия, предусмотренные договором.

Примеры: использование данных клиентов для выполнения заказов или данных контрагентов для исполнения условий договоров.

1.6.3 Выполнение юридических обязательств

Оператор обязан обрабатывать персональные данные для выполнения своих юридических обязательств, предусмотренных законодательством Российской Федерации или других юрисдикций, в которых ведется деятельность.

Обязательная обработка: Оператор обязан обрабатывать данные в соответствии с требованиями налогового, трудового, бухгалтерского законодательства и других нормативных актов. Например, это может включать хранение данных работников для целей налогового учета или предоставление данных государственным органам.

Минимизация данных: обработка данных в рамках выполнения юридических обязательств должна быть минимальной и соответствовать конкретным требованиям закона.

Примеры: хранение бухгалтерской документации, отчетов по налогам, регистрация работников в системе обязательного социального страхования.

1.6.4 Защита жизненно важных интересов субъекта данных

Персональные данные могут обрабатываться без согласия субъекта данных, если это необходимо для защиты его жизненно важных интересов, включая здоровье, безопасность и жизнь.

Экстренные ситуации: это основание используется в исключительных случаях, когда возникает угроза жизни или здоровью субъекта данных, и обработка данных необходима для оказания помощи, уведомления служб спасения или медицинских учреждений.

Минимизация вмешательства: обработка данных должна ограничиваться только теми сведениями, которые необходимы для защиты жизненно важных интересов субъекта данных.

Примеры: передача медицинских данных в случае несчастного случая или экстренной медицинской помощи, уведомление родственников в случае чрезвычайной ситуации.

1.6.5 Легитимные интересы Оператора

Персональные данные могут обрабатываться для целей легитимных интересов Оператора или третьих лиц, за исключением случаев, когда такие интересы нарушают права и свободы субъекта данных.

Баланс интересов: перед обработкой данных на основании легитимных интересов Оператор должен оценить баланс между своими интересами и правами субъекта данных. В случае, если интересы субъекта преобладают, обработка данных на этом основании недопустима.

Прозрачность: Оператор обязан информировать субъекта данных о том, что его данные обрабатываются на основании легитимных интересов, и предоставить информацию о характере этих интересов.

Примеры: использование данных для улучшения продуктов и услуг, защита интересов компании в судебных разбирательствах, обеспечение безопасности на предприятии.

2. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА - ООО «БАСФ»

Оператор обязуется действовать в строгом соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных», Регламента ЕС 2016/679 (GDPR), рекомендациями Роскомнадзора.

2.1. Права Оператора

2.1.1 Право на обработку персональных данных:

Оператор имеет право на обработку персональных данных субъектов в пределах, установленных законодательством Российской Федерации и международными нормами, для достижения целей, предусмотренных настоящей Политикой.

2.1.2 Право на получение персональных данных:

Оператор вправе запрашивать и получать от субъектов персональных данных или третьих лиц, представляющих интересы субъектов, персональные данные, необходимые для выполнения своих обязанностей и достижения целей обработки.

2.1.3 Право на передачу персональных данных:

Оператор имеет право передавать персональные данные третьим лицам (например,

аутсорсинговым компаниям, партнерам, государственным органам) при наличии законных оснований для такой передачи и в пределах, установленных законодательством.

2.1.4 Право на обезличивание и анонимизацию данных:

Оператор вправе проводить обезличивание и анонимизацию персональных данных для использования их в аналитических, статистических и иных законных целях, без возможности восстановления связи с конкретным субъектом данных.

2.1.5 Право на использование файлов cookie и аналогичных технологий:

Оператор вправе использовать файлы cookie и аналогичные технологии для улучшения работы сайтов, анализа поведения пользователей и персонализации предоставляемых услуг. Пользователи информируются о такой обработке и дают свое согласие в соответствии с требованиями законодательства.

2.1.6 Право на внесение изменений в Политику:

Оператор вправе вносить изменения и дополнения в настоящую Политику в любое время. Субъекты данных будут уведомлены о таких изменениях через соответствующие каналы связи (например, через веб-сайт компании).

2.2. Обязанности Оператора

2.2.1 Обеспечение законности обработки персональных данных:

Оператор обязан обрабатывать персональные данные в строгом соответствии с действующим законодательством Российской Федерации, международными стандартами (включая GDPR), а также настоящей Политикой.

2.2.2 Обеспечение безопасности персональных данных:

Оператор обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных от несанкционированного доступа, изменения, утраты или уничтожения. К таким мерам относятся:

- a. Шифрование данных и контроль доступа.
- b. Регулярные проверки и обновления систем безопасности.
- c. Назначение ответственных за обработку и защиту данных лиц.

2.2.3 Обеспечение конфиденциальности персональных данных:

Оператор обязан соблюдать конфиденциальность персональных данных, не допуская их раскрытия третьим лицам без правового основания, а также предотвратить несанкционированное распространение данных.

2.2.4 Получение согласия субъектов данных:

Оператор обязан получать явное согласие субъектов на обработку их персональных данных в случаях, предусмотренных законом. Также необходимо обеспечить субъектам возможность отзыва согласия в любой момент без ущерба для их прав.

2.2.5 Информирование субъектов данных:

Оператор обязан предоставлять субъектам персональных данных полную информацию о целях, способах, сроках обработки их данных, а также о правах субъектов данных в соответствии с законодательством и настоящей Политикой.

2.2.6 Уведомление надзорных органов о начале обработки:

Оператор обязан уведомлять уполномоченные органы (Роскомнадзор и другие) о намерении осуществлять обработку персональных данных, если это требуется по закону, а также поддерживать актуальность поданной информации.

2.2.7 Обеспечение прав субъектов персональных данных:

Оператор обязан уважать и обеспечивать права субъектов данных, включая право на доступ к данным, их исправление, удаление, ограничение обработки, а также право на перенос данных.

2.2.8 Реагирование на инциденты безопасности:

Оператор обязан немедленно реагировать на инциденты, связанные с утечкой или несанкционированным доступом к персональным данным, уведомлять об этом уполномоченные органы и субъектов данных, а также принимать меры по минимизации последствий таких инцидентов.

2.2.9 Обеспечение актуальности и достоверности персональных данных:

Оператор обязан предпринимать меры для поддержания персональных данных в актуальном и достоверном состоянии, включая регулярное обновление данных по мере необходимости или по запросу субъекта данных.

2.2.10 Уничтожение персональных данных:

Оператор обязан уничтожать персональные данные по истечении установленных сроков хранения или по достижении целей обработки, если иное не предусмотрено законодательством или договором с субъектом данных.

2.2.11 Документирование и хранение истории обработки данных:

Оператор обязан документировать процессы обработки персональных данных и сохранять историю изменений, включая получение согласий, передачу данных третьим лицам, инциденты безопасности и другие значимые события.

2.2.12 Взаимодействие с надзорными органами:

Оператор обязан сотрудничать с надзорными органами (например, Роскомнадзор) при проведении проверок и расследованиях инцидентов, связанных с обработкой персональных данных.

2.2.13 Обеспечение прозрачности обработки персональных данных:

Оператор обязан обеспечить прозрачность всех процессов обработки данных, предоставляя субъектам данных доступную и понятную информацию о том, как их данные собираются, используются и защищаются.

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ:**3.1. Поиск и подбор персонала**

цель: анализ предоставленной кандидатами информации, проведение собеседований и тестирований для оценки соответствия требованиям Оператора.

субъекты: кандидаты на замещение вакантных должностей.

правовые основания: согласие субъекта данных.

сроки обработки: до принятия решения о приеме на работу или отказе в трудоустройстве.

3.2. Управление кадровым резервом

цель: создание и поддержание актуальной базы данных перспективных кандидатов для будущих вакансий.

субъекты: работники и кандидаты на замещение вакантных должностей.

правовые основания: согласие субъекта данных.

сроки обработки: на протяжении времени нахождения кандидата в кадровом резерве.

3.3. Исполнение обязанностей работодателя

цель: исполнение обязанностей работодателя, предусмотренных трудовым законодательством Российской Федерации и иными актами, содержащими нормы трудового права, пенсионным и страховым законодательством Российской Федерации.

субъекты: работники, уволенные/уволившиеся работники.

правовые основания: Трудовой кодекс РФ, Налоговый кодекс РФ, иное применимое законодательство.

сроки обработки: определяются в зависимости от документа, содержащего персональные данные, в соответствии с приказом Росархива от 20.12.2019 № 236.

3.4. Организация обучения и повышения квалификации работников

цель: организация мероприятий по обучению и повышению квалификации, включая внутренние и внешние тренинги.

субъекты: работники.

правовые основания: Трудовой кодекс РФ, согласие субъекта данных.

сроки обработки: на период действия трудового договора.

3.5. Организация добровольного медицинского страхования

цель: заключение договоров добровольного медицинского страхования в отношении работников и указанных ими родственников.

субъекты: работники и их родственники.

правовые основания: согласие субъекта данных.

сроки обработки: на период действия трудового договора работника.

3.6. Оформление и организация командировок

цель: организация и оформление служебных командировок, включая бронирование билетов и размещения.

субъекты: работники.

правовые основания: Трудовой кодекс РФ, согласие субъекта данных.

сроки обработки: на период действия командировки.

3.7. Расчет и выплата заработной платы, вознаграждений и компенсаций

цель: обработка данных для расчета и выплаты заработной платы, бонусов и иных вознаграждений и компенсаций работникам.

субъекты: работники.

правовые основания: Трудовой кодекс РФ.

сроки обработки: на период действия трудового договора и 5 лет после его прекращения.

3.8. Управление налоговыми обязательствами

цель: обеспечение правильного расчета и уплаты налогов, взаимодействие с налоговыми органами.

субъекты: работники, контрагенты и их представители.

правовые основания: Налоговый кодекс РФ, обязательства по предоставлению данных в налоговые органы.

сроки обработки: до истечения срока действия договоров или налоговых обязательств.

3.9. Ведение переговоров, заключение и исполнение договоров

цель: проверка потенциальных контрагентов, заключение и исполнение договоров с контрагентами, включая оформление и отправку необходимой документации.

субъекты: контрагенты и их представители.

правовые основания: Гражданский кодекс РФ, ФЗ «О бухгалтерском учете», Налоговый кодекс РФ, выполнение договорных обязательств.

сроки обработки: на период действия договоров и 5 лет после прекращения их действия.

3.10. Управление цепями поставок и таможенным оформлением

цель: сопровождение заказов, таможенное оформление, оформление разрешительных документов.

субъекты: контрагенты и их уполномоченные представители, работники.

правовые основания: Гражданский кодекс РФ, Таможенный кодекс Евразийского экономического союза.

сроки обработки: на период действия договоров и 5 лет после прекращения их действия.

3.11. Оформление доверенностей

цель: предоставление полномочий для подписания документов и взаимодействия с органами государственной власти, органами местного самоуправления, судами, юридическими и физическими лицами.

субъекты: работники, контрагенты и их работники.

правовые основания: Гражданский кодекс РФ.

сроки обработки: в соответствии с приказом Росархива от 20.12.2019 № 236.

3.12. Управление подписками на новостные рассылки

цель: управление подписками пользователей на новостные и маркетинговые рассылки, отправка информационных и рекламных материалов.

субъекты: зарегистрированные пользователи Сайтов BASF, подписавшиеся на рассылки.

правовые основания: согласие субъекта данных.

сроки обработки: до отзыва согласия на получение рассылок.

3.13. Обработка запросов пользователей через онлайн-формы

цель: обработка запросов, предложений и вопросов, полученных через онлайн-формы на сайте, включая ответы и обратную связь пользователям.

субъекты: зарегистрированные пользователи Сайтов BASF.

правовые основания: согласие субъекта данных.

сроки обработки: на период обработки запроса и 1 год после завершения обработки.

3.14. Администрирование учетных записей пользователей

цель: создание и администрирование учетных записей пользователей на сайте, управление доступом к персонализированным услугам и контенту.

субъекты: зарегистрированные пользователи Сайтов BASF.

правовые основания: согласие субъекта данных, выполнение договорных обязательств.

сроки обработки: на период действия учетной записи и 1 год после ее деактивации.

3.15. Маркетинговая деятельность и управление отзывами клиентов

цель: сбор и анализ данных об опыте использования продукции, формирование рекламных и информационных предложений, размещение отзывов клиентов в публичных источниках.

субъекты: работники, контрагенты и их представители, лица, предоставлявшие отзывы.

правовые основания: согласие субъекта данных.

сроки обработки: до отзыва согласия или до завершения маркетинговой кампании.

3.16. Управление куки-файлами и технологиями отслеживания

цель: обработка данных пользователей через файлы cookie и аналогичные технологии для улучшения работы Сайтов BASF, предоставления персонализированного контента, а также для целей аналитики и рекламы.

субъекты: посетители и зарегистрированные пользователи Сайтов BASF.

правовые основания: согласие субъекта данных.

сроки обработки: в течение времени, необходимого для достижения целей, указанных при установке файлов cookie, или до отзыва согласия.

3.17. Создание внутреннего закрытого справочника

цель: обеспечение коммуникации между работниками.

субъекты: работники.

правовые основания: согласие субъекта данных.

сроки обработки: не более 30 календарных дней с момента прекращения действия договора.

4. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Эта глава детализирует порядок и условия обработки персональных данных в ООО «БАСФ», охватывая ключевые аспекты обработки данных, такие как автоматизированная и неавтоматизированная обработка, условия передачи данных третьим лицам, трансграничная передача, а также правила хранения, уничтожения и отзыва согласия на обработку данных.

4.1. Автоматизированная и неавтоматизированная обработка данных

Под автоматизированной обработкой понимается обработка персональных данных с использованием информационных технологий и программных средств, включая сбор, систематизацию, хранение, изменение, извлечение и передачу данных. Это включает в себя использование баз данных, CRM-систем, программ для обработки и анализа данных.

4.2. Неавтоматизированная обработка данных: осуществляется без использования информационных систем и программных средств. Это может включать работу с бумажными документами, карточками работников и другими физическими носителями информации.

Принципы безопасности: в обоих случаях обработка данных должна осуществляться с соблюдением требований безопасности, включая защиту от несанкционированного доступа, утраты и порчи данных.

Минимизация данных: Оператор обязан обрабатывать только те данные, которые необходимы для достижения целей, указанных в Политике, и минимизировать объем обрабатываемых данных.

Примеры:

Автоматизированная обработка: расчет заработной платы через специальное программное обеспечение.

Неавтоматизированная обработка: ведение бумажного архива трудовых договоров.

4.3. Условия передачи данных третьим лицам

Передача персональных данных третьим лицам возможна только в случаях, предусмотренных законодательством или с согласия субъекта данных. Передача данных должна осуществляться с соблюдением всех необходимых мер безопасности и конфиденциальности.

передача по закону: передача данных может быть осуществлена в случаях, предусмотренных законодательством, например, для выполнения судебного решения или по требованию государственных органов.

передача по договору: персональные данные могут быть переданы третьим лицам для выполнения договорных обязательств, например, контрагентам или подрядчикам, участвующим в исполнении договора.

защита данных: Оператор обязан убедиться, что третье лицо, которому передаются данные, обеспечивает их надлежащую защиту и использует данные только в целях, согласованных с субъектом данных.

пример: передача данных сервисной компании для предоставления услуг, предусмотренных договором.

4.4. Порядок трансграничной передачи данных

Трансграничная передача персональных данных — это передача данных на территорию иностранных государств. ООО «БАСФ» осуществляет такую передачу при соблюдении всех установленных законодательством условий.

4.4.1. Уведомление Роскомнадзора и согласие субъекта данных

Перед осуществлением трансграничной передачи персональных данных ООО «БАСФ» в обязательном порядке направляет уведомление в Роскомнадзор о намерении передать данные за пределы Российской Федерации. При этом отдельного согласия субъекта данных на осуществление трансграничной передачи данных не требуется.

4.4.2. Соблюдение стандартов защиты данных

Трансграничная передача данных осуществляется Оператором после подтверждения им соблюдения получателем данных установленных российским и международным законодательством стандартов.

4.4.3. Текущие направления трансграничной передачи данных

ООО «БАСФ» осуществляет трансграничную передачу персональных данных в Германию (BASF SE), которая считается страной с адекватным уровнем защиты данных. Это подтверждается соглашением, заключенным с BASF SE, которое включает все необходимые меры по защите данных.

4.5. Хранение и уничтожение персональных данных

Хранение и уничтожение персональных данных должны осуществляться в строгом соответствии с законодательством и внутренними нормативными актами компании.

сроки хранения: персональные данные должны храниться в течение сроков, определенных законодательством или внутренними нормативными актами компании. После истечения этих сроков данные должны быть уничтожены или обезличены.

методы уничтожения: уничтожение персональных данных должно производиться таким образом, чтобы исключить возможность их восстановления. Для этого могут использоваться специальные программные средства для удаления данных или физическое уничтожение носителей информации.

архивирование: в некоторых случаях данные могут быть архивированы в соответствии с требованиями законодательства, например, данные, связанные с бухгалтерской и финансовой отчетностью.

примеры: архивирование финансовой документации для целей налогового учета.

4.6. Порядок отзыва согласия на обработку данных

Субъект данных имеет право в любой момент отозвать свое согласие на обработку персональных данных. Оператор обязан обеспечить субъекту возможность реализации этого права без создания препятствий.

простота отзыва: Оператор обязан предоставить простой и доступный способ для отзыва согласия, например, через веб-форму на сайте или письменный запрос.

прекращение обработки: после получения запроса на отзыв согласия Оператор обязан немедленно прекратить обработку персональных данных субъекта, за исключением случаев, когда обработка может продолжаться на иных законных основаниях.

уведомление: Оператор обязан уведомить субъекта данных о прекращении обработки и об уничтожении или обезличивании его данных.

5. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Эта глава описывает меры, принимаемые ООО «БАСФ» для обеспечения безопасности персональных данных. Эти меры направлены на защиту данных от несанкционированного доступа, утраты, изменения или уничтожения, и соответствуют требованиям российского законодательства, а также международным стандартам, таким как GDPR.

5.1. Организационные меры

Организационные меры включают в себя создание и внедрение внутренних нормативных актов, процедур и инструкций, направленных на защиту персональных данных, а также назначение ответственных лиц за их обработку и защиту.

Основные меры:

назначение ответственного за защиту данных: определение ответственных лиц, включая назначение специалиста по защите данных, который контролирует соблюдение требований по обработке и защите данных.

регламентация доступа: разработка и внедрение документов, регулирующих доступ к персональным данным и их использование.

периодическое обучение работников: проведение тренингов и инструктажей для работников по вопросам защиты персональных данных и информационной безопасности.

аудиты и проверки: организация регулярных внутренних аудитов и проверок на соответствие требованиям законодательства и внутренних нормативных актов в области защиты данных.

5.2. Технические меры

Технические меры направлены на защиту информационных систем, в которых обрабатываются персональные данные, от несанкционированного доступа, утраты, изменения или уничтожения данных.

Основные меры:

шифрование данных: использование методов шифрования для защиты данных как при передаче, так и при хранении, чтобы предотвратить несанкционированный доступ.

защита сетей: внедрение межсетевых экранов, антивирусного ПО, систем обнаружения вторжений (IDS) и других технологий для защиты корпоративных сетей.

резервное копирование: регулярное создание резервных копий данных для обеспечения их сохранности и возможности восстановления в случае утраты.

обновление и патчинг: регулярное обновление программного обеспечения и установка патчей безопасности для устранения уязвимостей.

5.3. Контроль доступа к персональным данным

Контроль доступа предусматривает меры по ограничению доступа к персональным данным, чтобы они обрабатывались только теми работниками, которые имеют на это соответствующие полномочия.

Основные меры:

разграничение прав доступа: разделение прав доступа к персональным данным в зависимости от обязанностей работников, обеспечивая минимально необходимый доступ к данным.

аутентификация и авторизация: использование современных методов аутентификации (например, двухфакторной) и систем управления доступом для идентификации и проверки полномочий пользователей.

5.4. Меры по защите данных при передаче и хранении

Эти меры направлены на защиту персональных данных в процессе их передачи по сети, а также при хранении на серверах и других носителях информации.

защита каналов передачи данных: использование защищенных каналов связи, таких как vpn и шифрование данных при передаче через Интернет, для предотвращения их перехвата.

физическая безопасность: обеспечение защиты серверных помещений, архивов и других мест хранения данных с помощью видеонаблюдения, сигнализации и ограниченного доступа.

шифрование данных: хранение данных в зашифрованном виде на серверах и устройствах, чтобы обеспечить их защиту в случае утраты или кражи оборудования.

5.5. Обнаружение и реагирование на инциденты безопасности

Оператор обязан иметь процедуры и инструменты для обнаружения, расследования и реагирования на инциденты безопасности, связанные с утечкой или несанкционированным доступом к персональным данным.

Основные меры:

системы обнаружения вторжений (IDS): внедрение систем мониторинга, которые отслеживают подозрительную активность и предупреждают о возможных инцидентах безопасности.

план реагирования на инциденты: разработка и внедрение плана реагирования на инциденты, который включает действия по изоляции угрозы, уведомлению субъектов данных и уполномоченных органов, а также восстановление данных.

анализ и отчетность: проведение анализа причин инцидентов, составление отчетов и внедрение мер по предотвращению повторения аналогичных ситуаций в будущем.

6. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С СУБЪЕКТАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В этой главе описаны процедуры, которые ООО «БАСФ» применяет для взаимодействия с субъектами персональных данных, включая порядок обращения субъектов, рассмотрения их жалоб и запросов, а также взаимодействие с уполномоченными органами. Эти процедуры направлены на обеспечение прозрачности обработки данных и защиту прав субъектов.

6.1. Порядок обращения субъектов данных

Субъекты персональных данных имеют право направлять обращения в ООО «БАСФ» по вопросам, связанным с обработкой их персональных данных, включая запросы на доступ, исправление, удаление данных, а также иные запросы, касающиеся их прав.

форма обращения: обращения могут направляться в письменной форме, электронной почтой или через специальную форму на официальном сайте компании. ООО «БАСФ» обеспечивает доступность этих каналов для всех субъектов данных.

содержание обращения: обращение должно содержать информацию, необходимую для идентификации субъекта данных и его запроса, включая контактные данные, описание проблемы или запроса, а также документы, подтверждающие личность субъекта, если это необходимо.

сроки рассмотрения: Оператор обязан рассмотреть обращение субъекта данных и предоставить ответ в установленный срок, обычно не превышающий 30 календарных дней с момента получения обращения.

6.2. Порядок рассмотрения жалоб и запросов

ООО «БАСФ» обязано рассматривать жалобы и запросы субъектов персональных данных в соответствии с установленным порядком, обеспечивая своевременное и полное рассмотрение каждого обращения.

процедура обработки жалоб: жалобы и запросы субъектов данных регистрируются и передаются в соответствующее подразделение для рассмотрения. В случае необходимости могут быть проведены дополнительные проверки или консультации с ответственными лицами.

информирование субъекта данных: по результатам рассмотрения жалобы или запроса субъект данных информируется о принятых мерах и результатах в письменной или электронной форме. В случае отказа в удовлетворении запроса субъекту данных разъясняются причины отказа и порядок обжалования.

контроль и отчетность: ООО «БАСФ» ведет учет всех поступивших жалоб и запросов, а также принятых по ним мер. Эта информация используется для анализа и улучшения процедур взаимодействия с субъектами данных.

6.3. Взаимодействие с уполномоченными органами

ООО «БАСФ» взаимодействует с уполномоченными государственными органами (например, Роскомнадзором) в случаях, предусмотренных законодательством, для обеспечения соблюдения требований по защите персональных данных.

процедуры взаимодействия: в случае получения запросов от уполномоченных органов ООО «БАСФ» обязано предоставлять запрашиваемую информацию в установленные сроки и в полном объеме. Это может включать информацию о процедурах обработки данных, состоянии защиты данных и принятых мерах по устранению нарушений.

оповещение субъектов данных: если законодательство требует уведомления субъекта данных о взаимодействии с уполномоченными органами (например, в случае проверки или расследования), ООО «БАСФ» обязано своевременно проинформировать субъектов данных о таком взаимодействии.

сотрудничество и поддержка: ООО «БАСФ» обязано оказывать содействие уполномоченным органам при проведении проверок и расследований, а также предпринимать необходимые меры для устранения выявленных нарушений и предотвращения их повторения.

7. ЛОКАЛИЗАЦИЯ И ХРАНЕНИЕ ДАННЫХ. **ПЕРЕДАЧА ДАННЫХ ТРЕТЬИМ ЛИЦАМ**

Эта глава описывает порядок локализации и хранения персональных данных ООО «БАСФ» в соответствии с требованиями российского законодательства и международных стандартов.

7.1. Хранение данных на территории Российской Федерации

В соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных», все персональные данные граждан Российской Федерации, обрабатываемые ООО «БАСФ», должны храниться на территории Российской Федерации. Это требование касается как первичного сбора данных, так и их дальнейшей обработки и хранения.

Системы хранения: персональные данные должны храниться в базах данных и на серверах, расположенных на территории Российской Федерации. Это касается всех данных, собранных в рамках деятельности компании, включая данные работников, клиентов и контрагентов.

Резервные копии: резервные копии персональных данных также должны храниться на территории РФ, чтобы обеспечить соблюдение требований законодательства.²

7.2. Сроки хранения персональных данных

Персональные данные должны храниться только в течение того времени, которое необходимо для достижения целей обработки, указанных в Политике обработки персональных данных ООО «БАСФ». Сроки хранения данных зависят от характера данных и целей их обработки.

Минимизация срока хранения: персональные данные должны храниться только в течение времени, необходимого для выполнения договорных обязательств, соблюдения требований законодательства или других целей, указанных в Политике.

7.3. Условия уничтожения данных после завершения обработки

После достижения целей обработки или истечения сроков хранения, персональные данные должны быть уничтожены либо обезличены таким образом, чтобы исключить возможность восстановления и идентификации субъекта данных.

Методы уничтожения: уничтожение данных может быть осуществлено путем физического уничтожения носителей информации (бумажных документов) или с использованием специализированного программного обеспечения для удаления данных с электронных носителей.

Документирование уничтожения: все операции по уничтожению данных должны быть документально зафиксированы. Документы, подтверждающие уничтожение данных, должны содержать информацию о дате, методе уничтожения и лицах, ответственных за выполнение этой операции.

Уведомление субъекта данных: в случаях, когда уничтожение данных может затронуть права субъекта данных (например, при отзыве согласия на обработку данных), субъект должен быть уведомлен о факте и сроках уничтожения его данных.

7.4. Перечень третьих лиц, которым передаются персональные данные

1. АО «Райффайзенбанк»

цель передачи: открытие дебетовых карт для командировочных расходов работников и расчетов по ним.

объем передаваемых данных: ФИО, дата рождения, паспортные данные, адрес регистрации, номер телефона.

трансграничная передача: не осуществляется.

2. АО «Коммерцбанк (Евразия)»

цель передачи: выполнение расчетов с контрагентами.

объем передаваемых данных: ФИО, ИНН, банковские реквизиты.

трансграничная передача: не осуществляется.

3. ПАО «Сбербанк»

цель передачи: выполнение расчетов с работниками.

объем передаваемых данных: ФИО, ИНН, банковские реквизиты.

трансграничная передача: не осуществляется.

4. АО «Юникредит Банк»

цель передачи: выполнение расчетов с работниками.

объем передаваемых данных: паспортные данные, ФИО, ИНН, банковские реквизиты.

трансграничная передача: не осуществляется.

5. ООО «Альвист»

цель передачи: организация деловых поездок работников.

объем передаваемых данных: ФИО, паспортные данные, данные заграничного паспорта, дата рождения, телефон.

трансграничная передача: не осуществляется.

6. ООО «Юсиэмэс Групп»

цель передачи: оказание услуг по кадровому администрированию, расчету заработной платы и другим HR-услугам.

объем передаваемых данных: ФИО, табельный номер, ИНН, снилс, паспортные данные, адрес регистрации, контактные сведения, банковские реквизиты, семейное положение, данные о трудовой деятельности и доходах, а также данные ближайших родственников работников.

трансграничная передача: не осуществляется.

7. ООО «Один Клик»

цель передачи: обучение работников на сторонней платформе (электронные курсы).

объем передаваемых данных: ФИО, должность, подразделение, корпоративная почта.

трансграничная передача: не осуществляется.

8. ООО «Альтернатива-Консалтинформ»

цель передачи: проверка достоверности и полноты сведений о кандидатах на замещение вакантных должностей.

объем передаваемых данных: ФИО, дата рождения, место рождения, гражданство, паспортные данные, адрес регистрации, данные водительского удостоверения, контактные сведения, состав семьи, информация о трудовой деятельности, сведения о судимости, сведения об учете в наркологических или психоневрологических учреждениях.

трансграничная передача: не осуществляется.

9. BASF SE (Германия)

цель передачи: управление персоналом и их развитием, обеспечение организационной и хозяйственной деятельности Оператора, ведение взаиморасчетов работников с Оператором, обеспечение коммуникации между работниками Оператора и работниками группы компаний BASF.

объем передаваемых данных: ФИО, год рождения, занимаемая должность, подразделение, фотография, контактные сведения, пол, образование, дата рождения, доходы, реквизиты лицевого/банковского счета, место рождения.

трансграничная передача: осуществляется.

10. АО «АльфаСтрахование».

цель передачи: заключение договора добровольного медицинского страхования в интересах застрахованных лиц.

объем передаваемых данных: ФИО, дата рождения, адрес фактического проживания, номер контактного телефона, адрес электронной почты, степень родства с работником Оператора.

трансграничная передача: не осуществляется.

8. ОТВЕТСТВЕННОСТЬ И КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПОЛИТИКИ

8.1. Ответственные лица за обработку и защиту персональных данных

Ответственное лицо (DPO): назначается лицо, ответственное за организацию обработки персональных данных, который осуществляет контроль за соблюдением требований по защите данных, проводит регулярные оценки рисков и контролирует выполнение требований законодательства и внутренних регламентов.

Функции ответственного лица: организует обучение работников, контролирует доступ к персональным данным, обеспечивает реализацию прав субъектов данных и реагирует на инциденты, связанные с утечками или несанкционированным доступом к данным.

Взаимодействие с руководством: регулярно отчитывается перед руководством компании о текущем состоянии дел в области защиты данных и предлагаемых мерах по улучшению системы защиты данных.

8.2. Внутренние аудиты и проверки соблюдения Политики

Для обеспечения соблюдения Политики ООО «БАСФ» проводит внутренние аудиты и проверки, направленные на оценку эффективности системы защиты персональных данных и соответствие действующему законодательству.

Периодичность проверок: внутренние аудиты проводятся на регулярной основе, не реже одного раза в год, или по требованию уполномоченных органов.

Процедура аудита: аудиты включают проверку документации, контроль за соблюдением процедур обработки и защиты данных, оценку рисков и выявление уязвимостей в системе безопасности. Результаты аудитов документируются и доводятся до сведения руководства.

Корректирующие меры: в случае выявления нарушений по результатам проверок разрабатываются и внедряются корректирующие меры для устранения нарушений и улучшения системы защиты данных.

8.3. Ответственность за нарушение Политики

Работники и должностные лица ООО «БАСФ», ответственные за обработку и защиту персональных данных, несут персональную ответственность за соблюдение данной Политики и выполнение требований законодательства.

Дисциплинарная ответственность: за нарушение Политики или законодательства работники могут быть привлечены к дисциплинарной ответственности, включая замечания, выговоры или увольнение.

Материальная ответственность: в случае причинения ущерба «ООО «БАСФ» или субъектам данных в результате нарушения Политики, виновные лица могут быть привлечены к материальной ответственности в соответствии с трудовым законодательством и внутренними нормативными актами.

Административная и уголовная ответственность: в случаях, предусмотренных законодательством, за нарушения в области защиты персональных данных виновные лица могут быть привлечены к административной или уголовной ответственности.

9. ВНЕСЕНИЕ ИЗМЕНЕНИЙ И ПЕРЕСМОТР ПОЛИТИКИ

9.1. Процедура внесения изменений в Политику

Процедура внесения изменений в Политику обработки персональных данных направлена на своевременное обновление Политики в случае изменений законодательства, внутренних процессов «ООО «БАСФ» или требований к защите данных.

Инициатива изменений: инициировать внесение изменений в Политику может любое подразделение компании, ответственное за обработку персональных данных, а также лицо, назначенное ответственным за защиту данных (DPO).

Процесс утверждения: все предлагаемые изменения проходят этапы согласования и утверждения с руководством ООО «БАСФ». После согласования и принятия изменений Политика пересматривается и публикуется в актуализированном виде.

Юридическая экспертиза: внесенные изменения должны пройти юридическую экспертизу для обеспечения их соответствия требованиям законодательства.

9.2. Уведомление о внесении изменений

После внесения изменений в Политику обработки персональных данных, ООО «БАСФ» обязано уведомить субъектов данных о таких изменениях, особенно если они затрагивают права и обязанности субъектов данных.

Способы уведомления: уведомление осуществляется путем опубликования обновленной версии Политики на официальном сайте «ООО «БАСФ» и информирования по корпоративной электронной почте.

Сроки уведомления: уведомление субъектов данных должно быть осуществлено в разумные сроки, но не позднее 30 календарных дней с момента утверждения изменений.

9.3. Сроки пересмотра Политики

Политика пересматривается в случаях изменения законодательства в области обработки персональных данных, получения соответствующего предписания от уполномоченного органа, изменения процессов Оператора, связанных с обработкой персональных данных, а также по решению руководства.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

ООО «БАСФ» обязано обеспечить ознакомление всех работников с актуальной версией Политики обработки персональных данных.

10.1. Ознакомление при приеме на работу: каждый новый работник компании должен быть ознакомлен с Политикой обработки персональных данных в рамках процедур приема на работу. Факт ознакомления подтверждается письменной подписью работника или через электронные системы документооборота.

10.2. Публичность Политики

Политика обработки персональных данных ООО «БАСФ» доступна для ознакомления как работникам компании, так и любым заинтересованным лицам, включая субъектов персональных данных и контролирующие органы.

Размещение на сайте: актуальная версия Политики должна быть размещена на официальном веб-сайте компании, чтобы все заинтересованные лица могли свободно ознакомиться с ней. На сайтах BASF могут быть размещены дополнительные документы – соответствующие Политики конфиденциальности, являющиеся частью настоящей Политики и описывающие только процессы обработки персональных данных пользователей сайтов.

Зам Ген. Директора

О. В. Бочков

ООО «БАСФ» по ОТ и ПБ