Открытое акционерное УТВЕРЖДЕНО

общество «МЗОР» Приказ директора общества

27.11.2023 № 150

ПОЛОЖЕНИЕ

Об обработке и защите

персональных данных

ГЛАВА 1

ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее положение разработано в соответствии с Конституцией Республики Беларусь, Трудовым кодексом Республики Беларусь, Гражданским кодексом Республики Беларусь, Законом Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных», Законом Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации», иными нормативными правовыми актами Республики Беларусь.

2. Настоящее положение является локальным правовым актом и определяет правила обработки персональных данных, меры по обеспечению режима их защиты, обязанности и ответственность лиц, осуществляющих обработку персональных данных в ОАО «МЗОР» (далее – Общество, Оператор).

3. Требования настоящего положения обязательны для исполнения сотрудниками Общества, имеющими доступ к персональным данным.

4. Действие настоящего положения не распространяется на отношения, касающиеся случаев обработки персональных данных:

физическими лицами в процессе исключительно личного, семейного, домашнего и иного подобного их использования, не связанного с профессиональной или предпринимательской деятельностью;

отнесенных в установленном порядке к государственным секретам.

5. Настоящее положение функционально работает совместно с политикой в отношении обработки персональных данных (далее – политика) и иными локальными правовыми актами Общества.

6. В настоящем положении используются следующие основные термины и их определения:

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств автоматизации;

блокирование персональных данных – прекращение доступа к персональным данным без их удаления;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и информационных технологий и технических средств, обеспечивающих их обработку;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных к конкретному субъекту персональных данных;

обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемыми с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;

обработка персональных данных без использования средств автоматизации – действие, которое обеспечивает поиск и (или) доступ к ним по определенным критериям (картотеки, списки, базы данных, журналы и другое);

оператор персональных данных – ОАО «МЗОР»;

персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано;

предоставление персональных данных – действия, направленные на ознакомление с персональными данными определенных лиц или круга лиц;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

средства автоматизации – совокупность технических и программных средств, предназначенных для сбора, ввода, обработки, хранения, отображения, регистрации и документирования информации, а также для обмена данными в информационных сетях и системах;

лицо ответственное за осуществление внутреннего контроля за обработкой персональных данных – начальник управления безопасности и охраны объекта;

субъект персональных данных – физическое лицо, в отношении которого осуществляется обработка персональных данных;

специалист – работник оператора, который в силу своих трудовых обязанностей обрабатывает персональные данные;

трансграничная передача персональных данных – действия по их передаче на территорию иностранного государства (сервер, на который передаются персональные данные, физически находится в иностранном государстве);

удаление персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

ГЛАВА 2

ТРЕБОВАНИЯ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7. При обработке персональных данных специалист, имеющий доступ к обработке персональных данных, должен соблюдать следующие требования:

обрабатывать персональные данные в целях, определенных политикой. Не допускается запрашивать сведения, которые оператору не понадобятся;

обрабатывать персональные данные с согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством;

обработка персональных данных должна носить прозрачный характер;

  принимать меры по обеспечению достоверности обрабатываемых им персональных данных: проверять предоставленные персональные данные, запрашивать персональные данные, а также при необходимости вносить изменения в персональные данные, хранящиеся у него;

хранить персональные данные не дольше, чем этого требуют цели, для которых они собраны.

ГЛАВА 3

ПРАВИЛА ОБРАБОТКИ И ЗАЩИТЫ

ПЕРСОНАЛЬНЫХ ДАННЫХ

8. Согласие на обработку персональных данных.

Специалист ведет обработку персональных данных путем смешанной (как с использованием средств автоматизации, так и без использования средств автоматизации) обработки, в том числе с использованием внутренней сети и сети Интернет.

Перед началом обработки персональных данных специалист истребует письменное согласие соответствующего субъекта персональных данных в зависимости от цели обработки персональных данных.

Согласие субъекта персональных данных на обработку данных может быть получено на интернет - ресурсе оператора путем проставления отметки (галочки) напротив текста о предоставлении согласия на обработку персональных данных на сайте.

Письменное согласие субъекта персональных данных на обработку его персональных данных должно включать в себя:

фамилию, собственное имя, отчество (если таковое имеется);

дату рождения;

идентификационный номер, а в случае отсутствия такого номера, номер документа, удостоверяющего его личность;

подпись субъекта персональных данных.

При этом специалист предоставляет субъекту персональных данных следующую информацию:

наименование и место нахождение организации, которой необходимы персональные данные физического лица;

цели обработки персональных данных;

перечень персональных данных, на обработку которых дается согласие физического лица;

срок, на который физическое лицо дает согласие на обработку персональных данных.

После получения согласия специалист разъясняет физическому лицу права, связанные с обработкой его персональных данных, механизм реализации таких прав, а также последствия предоставления согласия или отказа в даче такого согласия (приложение 2 приказа от 18.01.2022 №55 «Об утверждении Политики в отношении обработки персональных данных»).

Согласие субъекта персональных данных на обработку его персональных данных, за исключением специальных персональных данных, не требуется в случаях, предусмотренных статьей 6 Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».

Оператором не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством Республики Беларусь.

9. Сбор персональных данных.

Специалист получает персональные данные субъекта персональных данных:

от самого субъекта персональных данных;

от третьих лиц только при наличии письменного согласия субъекта на получение его персональных данных от третьих лиц, если иное не установлено Законом Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных»;

при ведении оператором видеонаблюдения, в том числе с функцией аудиозаписи, организованного в административных зданиях, в производственных и складских помещениях, на контрольно-пропускных пунктах, по периметру предприятия, осуществляемого с целью: обеспечения производственно-технологической, исполнительской и трудовой дисциплины; ведения учета фактически отработанного работниками времени; ведения контроля за соблюдением работниками на каждом рабочем месте требований по охране труда; предотвращения хищения, порчи, уничтожения материальных ценностей.

В зданиях, где ведется видеонаблюдение, в том числе с аудиозаписью, должны быть установлены соответствующие предупреждающие знаки (таблички).

Оператором ЭВМ (по видеонаблюдению) является сотрудник службы информационных технологий, для которого обязанность по обработке материалов видеонаблюдения содержится в должностной (рабочей) инструкции.

Доступ к материалам видеонаблюдения имеют сотрудники управления безопасности и охраны объекта (далее – УБиОО). Доступ к материалам видеонаблюдения иным работникам Общества осуществляется только по согласованию с начальником УБиОО.

Материалы видеонаблюдения хранятся на серверном оборудовании оператора не более 90 календарных дней. При необходимости срок хранения таких материалов может быть продлен по решению руководителя оператора.

10. Хранение персональных данных.

При хранении персональных данных специалист должен соблюдать условия, обеспечивающие сохранность персональных данных.

Специалист хранит документы, включающие в себя персональные данные, содержащиеся на бумажных носителях, в сейфах, несгораемых шкафах, шкафах с запирающими устройствами, исключающих доступ к ним посторонних лиц.

Персональные данные, хранящиеся в электронном виде, защищаются от несанкционированного доступа с помощью специальных технических и программных средств защиты.

Программные средства защиты информации включают в себя:

средства криптографической защиты информации;

антивирусные программы;

средства идентификации и аутентификации пользователей;

средства управления доступом;

средства протоколирования и аудита и т.д.

Доступ в помещения, в которых размещены информационные системы, в том числе содержащие персональные данные, имеют лишь сотрудники службы информационных технологий.

Специалист осуществляет хранение персональных данных в электронном виде в тех информационных системах, к которым имеет доступ (пароль). Передача пароля другим лицам запрещается.

Хранение персональных данных в электронном виде вне применяемых оператором информационных систем и специально обозначенных оператором баз данных (внесистемное хранение персональных данных) не допускается.

Хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта персональных данных, но не дольше, чем этого требуют цели их обработки, если иной срок не установлен законодательством Республики Беларусь или договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

11. Использование персональных данных.

Специалист обрабатывает и использует персональные данные для целей, указанных в главе 3 политики в отношении обработки персональных данных.

Доступ к обработке персональных данных предоставляется только тем специалистам, в служебные обязанности которых входит работа с персональными данными.

Специалист обрабатывает и использует персональные данные только на период, необходимый для работы с соответствующими данными.

В случае возникновения необходимости работнику может быть предоставлен временный доступ к ограниченному кругу персональных данных по распоряжению руководителя подразделения, согласованного с начальником УБиОО. Соответствующие работники должны быть ознакомлены под подпись со всеми локальными правовыми актами оператора в области персональных данных.

Работникам оператора, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным запрещается.

12. Передача персональных данных.

Специалист передает персональные данные третьим лицам в минимально необходимых объемах и только в целях выполнения задач, соответствующих объективным целям сбора этих данных.

Передача персональных данных третьим лицам, в том числе в коммерческих целях, допускается при наличии согласия субъекта, за исключением случаев, предусмотренных законодательством Республики Беларусь.

Передача информации, содержащей персональные данные, должна осуществляться способом, обеспечивающим защиту от неправомерного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий в отношении такой информации.

В случае необходимости трансграничной передачи персональных данных специалист уведомляет об этом начальника УБиОО.

При трансграничной передаче персональных данных начальник УБиОО обязан:

проверить на включение иностранного государства, на территорию которого планируется передача персональных данных, в перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных;

запрашивать разрешение на трансграничную передачу персональных данных у уполномоченного органа по защите прав субъектов персональных данных, если иностранное государство не входит в перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных;

истребовать у субъекта персональных данных согласие (несогласие) на трансграничную передачу персональных данных, если иностранное государство не входит в перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных и отсутствуют условия, предусмотренные в абз. 3-8 п. 1 ст. 9 Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (Приложение 1).

В случаях, когда государственные органы имеют право запросить персональные данные или персональные данные должны быть предоставлены на основании законодательства Республики Беларусь, а также в соответствии с запросом суда, правоохранительных органов и т.д., соответствующая информация может быть им предоставлена в порядке, предусмотренном действующим законодательством Республики Беларусь.

Все поступающие запросы от третьих лиц, государственных органов на выдачу персональных данных субъектов передаются начальнику УБиОО для предварительного рассмотрения и согласования.

13. Изменение персональных данных.

Специалист вносит изменения в персональные данные:

по требованию уполномоченного органа по защите прав субъектов персональных данных в связи с недостоверными данными;

по заявлению субъекта персональных данных.

Субъект персональных данных подает заявление об изменении персональных данных в письменной форме либо в виде электронного документа Оператору, в котором указывает: фамилия, собственное имя, отчество (если таковое имеется), адрес места жительства (регистрации); дату рождения, идентификационный номер, при отсутствии такого, номер документа, удостоверяющего личность; суть изменений.

Заявление подписывается субъектом персональных данных собственноручно либо с помощью электронной цифровой подписи.

К заявлению должны быть приложены документы или заверенные в установленном порядке копии, которые подтверждают такую необходимость.

Специалист обязан в 15-дневный срок:

внести соответствующие изменения в персональные данные;

уведомить начальника УБиОО о внесении соответствующих изменений или об отказе во внесении изменений.

В свою очередь начальник УБиОО уведомляет субъект персональных данных о внесении или об отказе внесения изменений в персональные данные.

14. Блокирование, обезличивание и уничтожение персональных данных.

Начальник УБиОО блокирует персональные данные в случае:

получения от субъекта персональных данных заявления об отзыве своего согласия на их обработку;

получения от субъекта персональных данных заявления о прекращении обработки персональных данных, но нет технической возможности их удалить;

выявления неточности внесенные в персональные данные;

по требованию уполномоченного органа по защите прав субъектов персональных данных в связи с их недостоверностью либо получением оператором данных незаконным путем.

Срок блокирования персональных данных составляет 15 дней после получения соответствующего заявления субъекта персональных данных.

Начальник УБиОО дает поручение специалисту, обрабатывающему персональные данные, об их уничтожении или обезличивании в случае поступления от субъекта персональных данных заявления (обращения) о прекращении обработки данных (их удалении).

Специалист по достижении целей обработки персональных данных, в случае утраты необходимости в достижении целей обработки персональных данных или по истечении сроков их хранения уничтожает персональные данные, о чем уведомляет начальника УБиОО.

Уничтожение или обезличивание персональных данных должно производиться способом, исключающим дальнейшую обработку этих персональных данных.

ГЛАВА 4

КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПРАВИЛ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

15. Мониторинг за соблюдением правил обработки и защиты персональных данных выполняет начальник УБиОО.

16. Начальник УБиОО:

ведет реестр обработки данных, в который вносятся изменения по мере необходимости, но не реже 1 раза в год.

осуществляет прием и обработку обращений и запросов субъектов персональных данных или их представителей (об отзыве согласия на обработку персональных данных, о получении информации об обработке данных, о внесении изменений в персональные данные, о получении информации о предоставлении данных третьим лицам, о прекращении обработки данные, их удалении) согласно журналу учета обращений (запросов) субъектов персональных данных (Приложение 2);

уведомляют субъектов персональных данных об устранении допущенных нарушений при обработке их персональных данных;

осуществляют блокирование персональных данных;

осуществляют внутренний контроль за соблюдением оператором и его работниками законодательства Республики Беларусь о персональных данных, в том числе требований к защите персональных данных;

доводит до сведения работников оператора правовую информацию Республики Беларусь о персональных данных, локальных правовых актов по вопросам обработки персональных данных, требований к защите персональных данных;

ограничивает и регламентирует состав работников, в функциональные обязанности которых входит доступ к информации, содержащей персональные данные (в том числе путем использования паролей доступа к электронным информационным ресурсам);

организует порядок уничтожения, обезличивая персональных данных, размещенных в информационных источниках;

обеспечивает возможность восстановления персональных данных модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

обнаруживает факты несанкционированного доступа к персональным данным и принимают меры реагирования;

проводит расследование случаев несанкционированного доступа или разглашения персональных данных и готовит документы для привлечения виновных лиц к ответственности или принимают иные меры воздействия;

обеспечивает сохранность носителей с информацией, включающей персональные данные;

осуществляет иные функции, направленные на организацию внутреннего контроля за соблюдением оператором и его работниками законодательства Республики Беларусь о персональных данных.

17. Начальник УБиОО при получении заявления субъекта персональных данных о прекращении обработки персональных данных в связи с отзывом согласия на их обработку; о внесении изменений в свои персональные данные; о получении информации о предоставлении персональных данных третьим лицам; о прекращении обработки персональных данных, включая их удаление осуществляет его рассмотрение в пятнадцатидневный срок.

Заявление субъекта персональных данных о получении информации, касающейся обработки персональных данных должно быть рассмотрено начальником УБиОО в течение пяти рабочих дней.

Заявление должно содержать:

фамилию, собственное имя, отчество (если таковое имеется) субъекта персональных данных, адрес его места жительства (места пребывания);

дату рождения субъекта персональных данных;

идентификационный номер субъекта персональных данных, при отсутствии такого номера, номер документа, удостоверяющего личность субъекта персональных данных, в случаях, если эта информация указывалась субъектом персональных данных при даче своего согласия оператору или обработка персональных данных осуществляется без согласия субъекта персональных данных;

изложение сути требований субъекта персональных данных;

личную подпись либо электронную цифровую подпись субъекта персональных данных.

Заявление может быть направлено в письменной форме по месту нахождения оператора, в форме электронного документа, подписанного электронной цифровой подписью в соответствии с законодательством Республики Беларусь на электронный адрес оператора, указанный в политике.

Если в заявлении субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Субъекту персональных данных может быть отказано в предоставлении информации в соответствии с частью 3 статьи 11 Закона о персональных данных.

18. При нарушении систем защиты персональных данных начальник УБиОО направляет в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

Уведомление не направляется, если нарушение систем защиты не привело к:

незаконному распространению, предоставлению персональных данных;

изменению, блокированию либо удалению персональных данных без возможности восстановления доступа к ним.

Уведомление направляется незамедлительно, но не позднее трех рабочих дней после того, как оператору стало известно о таких нарушениях, в письменной форме или в виде электронного документа.

Уведомление излагается на белорусском или русском языке и должно содержать:

полное наименование и место нахождения оператора (государственного органа, юридического лица Республики Беларусь, иной организации), а также номер телефона, адрес электронной почты (при наличии) оператора;

фамилию, собственное имя, отчество (если таковое имеется), должность лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных оператора;

дату и время нарушения системы защиты персональных данных;

дату и время, когда стало известно о произошедшем нарушении системы защиты персональных данных;

описание нарушения системы защиты персональных данных;

примерное количество субъектов персональных данных, затронутых нарушением;

вероятные неблагоприятные последствия нарушения системы защиты персональных данных (потеря контроля над персональными данными, их хищение, нарушение прав и свобод субъектов персональных данных, чести, достоинства или деловой репутации, наступление убытков, разглашение охраняемой законом тайны, наступление иного существенного имущественного или иного вреда у субъектов персональных данных);

меры, принятые или предлагаемые к принятию оператором для устранения нарушения системы защиты персональных данных.

ГЛАВА 5

ОТВЕТСТВЕННОСТЬ

19. Специалисты оператора, виновные в нарушении законодательства Республики Беларусь по обработке персональных данных и настоящего положения, несут ответственность, предусмотренную законодательством Республики Беларусь

20. Работники и иные лица, виновные в нарушении настоящего положения, а также законодательства Республики Беларусь в области персональных данных, могут быть привлечены к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Республики Беларусь, а также могут быть привлечены к гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством Республики Беларусь.

|  |
| --- |
|  |

Приложение 1

к положению об обработке и защите персональных данных

|  |  |  |
| --- | --- | --- |
| |  | | --- | | ЗАЯВЛЕНИЕ  о согласии (несогласии)  на трансграничную передачу персональных данных | | ОАО «МЗОР»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(наименование оператора)*  *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*  *(фамилия, собственное имя, отчество (если таковое имеется) субъекта персональных данных)*  *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*  *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*  *(номер документа, удостоверяющего личность, кем, когда выдан, идентификационный номер,*  *адрес)* |

Даю согласие (не согласен (-а)) на трансграничную передачу следующих персональных данных: *Фамилия Имя Отчество, дата рождения, место жительства, данные документа удостоверяющего личность,* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(перечислить персональные данные, на обработку которых дает согласие субъект персональных данных)*

с целью *осуществления необходимых мероприятий, связанных с моим командированием и пребыванием за границей при выполнении служебного задания*

*(указать цель)*

Оператором: *ОАО «МЗОР», г. Минск, ул. Ленина, 46 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(наименование, адрес оператора, получающего согласие субъекта персональных данных)*

на территорию иностранного государства, не обеспечивающего надлежащий уровень защиты прав субъектов персональных данных, в форме:

*в электронном форме через государственную границу Республики Беларусь органу власти иностранного государства, физическому или юридическому лицу иностранного государства*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(способы трансграничной передачи персональных данных)*

в период с настоящего момента и до истечения сроков действия трудового договора (контракта), в соответствии со ст. 9 Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» заявляю.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_.\_\_\_\_\_\_\_.20\_\_\_ |  |  |  |
|  | *(подпись)* |  | *(расшифровка подписи)* |

Мне разъяснены права, связанные с обработкой персональных данных, механизм их реализации прав, а также последствия дачи мною согласия или отказа в даче такого согласия.

С перечнем иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных ознакомлен.

Настоящее согласие может быть отозвано на основании письменного заявления субъекта персональных данных.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_.\_\_\_\_\_\_\_.20\_\_\_ |  |  |  |
|  | *(подпись)* |  | *(расшифровка подписи)* |

Перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных:

|  |  |
| --- | --- |
| 1. [Австрия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=AUS) 2. [Азербайджан](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=AZE) 3. [Албания](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=ALB) 4. [Андорра](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=AND) 5. [Аргентина](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=ARG) 6. [Армения](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=ARM) 7. [Бельгия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=BEL) 8. [Болгария](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=BUL) 9. [Босния и Герцеговина](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=BOS) 10. [Великобритания](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=UK) 11. [Венгрия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=HUN) 12. [Германия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=GER) 13. [Греция](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=GRE) 14. [Грузия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=GEO) 15. [Дания](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=DEN) 16. [Ирландия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=IRE) 17. [Исландия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=ICE) 18. [Испания](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=SPA) 19. [Италия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=ITA) 20. Казахстан 21. Кыргызстан 22. [Кабо-Верде](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=CAP) 23. [Кипр](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=CYP) 24. [Латвия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=LAT) 25. [Литва](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=LIT) 26. [Лихтенштейн](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=LIE) 27. [Люксембург](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=LUX) 28. [Мальта](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=MAL) 29. [Монако](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=MON) 30. [Нидерланды](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=NET) | 1. [Норвегия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=NOR) 2. [Остров Маврикий](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=MAU) 3. [Польша](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=POL) 4. [Португалия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=POR) 5. [Республика](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=MOL) Молдова 6. [Румыния](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=ROM) 7. [Сан-Марино](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=SAN) 8. [Северная Македония](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=TFY) 9. [Сербия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=SAM) 10. [Словацкая Республика](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=SLK) 11. [Словения](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=SLO) 12. [Турция](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=TUR) 13. [Украина](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=U) 14. [Финляндия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=FIN) 15. [Франция](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=FRA) 16. [Хорватия](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=CRO) 17. [Черногория](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=MOT) 18. [Чешская республика](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=CZE) 19. [Швейцария](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=SWI) 20. [Швеция](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=SWE) 21. [Эстония](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=EST) 22. [Марокко](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=MOR) 23. [Мексика](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=MEX) 24. Российская Федерация 25. [Сенегал](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=SEN) 26. [Тунис](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=TUN) 27. [Уругвай](https://www.coe.int/ru/web/conventions/full-list?module=treaties-full-list-signature&CodePays=URU) |

Приложение 2

к положению об обработке и защите персональных данных

ЖУРНАЛ

учета обращений (запросов) субъектов персональных данных

открытого акционерного общества «МЗОР»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Фамилия, Имя, Отчество (если таковое имеется) субъекта персональных данных | Дата обращения (запроса) | Суть запроса | Дата и номер ответа на обращение (запрос) | Примечание |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

иложение 2

к положению об обработке и защите персональных данных

от «\_\_\_»\_\_\_\_\_\_\_\_2023 №\_\_\_