Приложение 1

УТВЕРЖДЕНО приказом
от 12.03.2024г. № НТР/033-п

Положение

об обработке и обеспечении безопасности персональных данных в ООО «Н ТРЭВЕЛ»

Обозначение документа:
Введено взамен: № ТАВС/151-п от 26.12.2022
Дата введения: 12.03.2024

Содержание

1. Область применения

1.1. Настоящее Положение об обработке и обеспечении безопасности персональных данных в ООО «Н ТРЭВЕЛ» (далее – Положение) устанавливает единые правила для процессов обработки персональных данных и обеспечения безопасности персональных данных (далее - ПДн) в ООО «Н ТРЭВЕЛ» (далее - Общество). Положение устанавливает требования к:

1.1.1. Порядку обработки ПДн в части:

- автоматизированной обработки ПДн;
- неавтоматизированной обработки ПДн.

1.1.2. Особенностям передачи ПДн.

1.1.3. Особенностям удаления, уничтожения и обезличивания ПДн.

1.1.4. Порядку взаимодействия и Общества субъектами ПДн.

1.1.5. Порядку взаимодействия Общества с органами государственной власти по вопросам обработки ПДн и обеспечения безопасности ПДн.

1.1.6. Повышению осведомленности работников и иных лиц, допущенных к обработке ПДн.

1.1.7. Обеспечению безопасности ПДн.

1.1.8. Проведению оценки вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон 152-ФЗ).

1.1.9. Контролю за соблюдением требований в области обработки и защиты ПДн.

1.2. Целью разработки Положения является обеспечение исполнения требований законодательства Российской Федерации в области ПДн при обработке ПДн в Обществе, а также предотвращение и минимизация потенциального ущерба в случае нарушения конфиденциальности, целостности и доступности ПДн, обрабатываемых в Обществе.

1.3. Настоящее Положение не применяется к:

1.3.1. Организации хранения, комплектования, учета и использования содержащих ПДн архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.

1.3.2. Обработке ПДн, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.4. Требования настоящего Положения распространяются на всех работников Общества, участвующих в процессах обработки и обеспечении безопасности ПДн.

2. Общие положения

2.1. Основные принципы и условия обработки ПДн в Обществе установлены Политикой ООО «Н ТРЭВЕЛ» в области обработки персональных данных».

2.2. В Обществе ведется Перечень подлежащих обработке ПДн Общества (далее – Перечень ПДн) с учетом целей обработки ПДн, соответствующим деятельности, при которой такая обработка осуществляется.

2.3. В Обществе утверждается перечень лиц, доступ которых к ПДн, обрабатываемым в информационных системах персональных данных (далее – ИСПДн), необходим для выполнения ими трудовых обязанностей, а также лиц, осуществляющих неавтоматизированную обработку ПДн (далее – Перечень лиц, допущенных к обработке ПДн). Перечень лиц, допущенных к обработке ПДн в Обществе утверждается Генеральным директором Общества или уполномоченным им лицом. Перечень лиц, допущенных к обработке ПДн в Обществе, утверждается руководителем Общества или уполномоченным им лицом.

3. Структура и окружение системы управления ПДн

3.1. Система управления ПДн включает:

- обработку ПДн;
- взаимодействие Общества с субъектами ПДн;
- взаимодействие Общества с органами государственной власти по вопросам обработки ПДн и обеспечения безопасности ПДн;
- повышение осведомленности работников и иных лиц, допущенных к обработке ПДн;
- обеспечение безопасности ПДн;
- проведение оценки вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона 152-ФЗ;
- контроль за соблюдением требований в области обработки и защиты ПДн.

4. Функции участников

4.1. С целью организации, контроля обработки и обеспечения безопасности ПДн в Обществе определены следующие участники:

- Ответственный за организацию обработки ПДн в Обществе (п. 4.3 настоящего Положения);
- Ответственные за обеспечение безопасности ПДн в Обществе(п. 4.5 настоящего Положения);
- Подразделения, обеспечивающие эксплуатацию ИСПДн и ИТ-инфраструктуры в Обществе(п. 4.7 настоящего Положения);
- Подразделения, обеспечивающие эксплуатацию системы защиты ПДн (далее – СЗПДн) в Обществе(п. 4.7 настоящего Положения);
- Менеджеры безопасности ПДн при их обработке в ИСПДн в Обществе(п. 4.8 настоящего Положения);
- Менеджеры обработки ПДн в Обществе(п. 4.11 настоящего Положения);
- Работники правовых служб Общества (п. 4.13 настоящего Положения);
- Работники кадровых служб Общества (п. 4.14 настоящего Положения);
- Пользователи ПДн в Обществе(п. 4.15 настоящего Положения);
- Комиссия по обеспечению безопасности ПДн в Обществе (п. 4.17 настоящего Положения);
- Подразделение, организующее опубликование информации об условиях обработки ПДн в Обществе(п. 4.20 настоящего Положения).

4.2. Приказом Генерального директора Общества могут быть предусмотрены дополнительные участники процессов обработки и обеспечения безопасности ПДн в соответствующем подразделении Общества.

4.3. Ответственный за организацию обработки ПДн в Обществе назначается приказом Генерального директора Общества.

4.4. Функции Ответственного за организацию обработки ПДн в Обществе установлены Политикой ООО «Н ТРЭВЕЛ» в области обработки персональных данных.

4.5. Ответственные за обеспечение безопасности ПДн в Обществе назначаются распорядительным документом Генерального директора или уполномоченного им лица.

4.6. Функции Ответственных за обеспечение безопасности ПДн в Обществе установлены Политикой ООО «Н ТРЭВЕЛ» в области обработки персональных данных.

4.7. Подразделения, обеспечивающие эксплуатацию ИСПДн и ИТ-инфраструктуры в Обществе, выполняют следующие функции:

– предоставление сведений Менеджеру безопасности ПДн при их обработке в ИСПДн в Обществе для классификации информационных систем (далее – ИС) как ИСПДн, включая структурно-функциональные характеристики ИСПДн, сведения об информационно-интеграционном взаимодействии, архитектуре и функционировании ИС и сетей, внешних и внутренних интерфейсам взаимодействия, лицах, ответственных за обеспечение эксплуатации ИСПДн и ИТ-инфраструктуры;

– обеспечение работы ИСПДн в соответствии с РМД Общества и эксплуатационной документацией;

– управление доступом Пользователей ПДн в Обществе к ИСПДн;

– обеспечение наличия средств межсетевого экранирования;

– управление информационными (интеграционными) потоками между ИСПДн;

– реализация защищенного доступа к ИСПДн;

– участие в определении ключевых параметров ИСПДн (категории обрабатываемых ПДн, типы субъектов ПДн, которым принадлежат обрабатываемые ПДн, количество субъектов ПДн, ПДн которых обрабатываются в ИСПДн, типы актуальных угроз безопасности ПДн) и поддержание в актуальном состоянии описательной документации для них, в том числе паспорта ИС;

– участие в определении актуальных угроз безопасности ПДн для каждой ИСПДн;

– выполнение требований по безопасности ПДн при их обработке на серверном оборудовании ИСПДн;

– контроль доступа к техническим средствам ИСПДн;

– контроль перемещений серверных компонентов ИСПДн;

– обеспечение установки средств антивирусной защиты;

– организация резервирования ПДн и ИСПДн;

– управление установкой (инсталляцией) компонентов программного обеспечения (далее – ПО), в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО, установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов;

– контроль состава ИСПДн и ИТ-инфраструктуры;

– закрытие уязвимостей информационной безопасности (далее – ИБ) ИСПДн;

– обеспечение работоспособности, контроль параметров настройки и правильности функционирования ИСПДн и ИТ-инфраструктуры;

– обеспечение целостности информации в ИСПДн и ИТ-инфраструктуры;

– обеспечение доступности ИСПДн и ИТ-инфраструктуры, включая обеспечение доступности ИСПДн и ИТ-инфраструктуры в соответствии с бизнес-требованиями, выраженными параметрами RTO/RPO, контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и периодическое резервное копирование ПДн;

– управление конфигурацией ИСПДн и ИТ-инфраструктуры.

4.8. Подразделения, обеспечивающие эксплуатацию СЗПДн в Обществе, выполняют следующие функции:

– эксплуатация средств защиты информации, входящих в СЗПДн;

– эксплуатация средств контроля информационных потоков между ИСПДн;

– обеспечение работоспособности и правильности функционирования СЗИ;

– эксплуатация средств контроля взаимодействий с ИС сторонних организаций;

– управление доступом к машинным носителям ПДн и контроль подключения машинных носителей ПДн;

– эксплуатация средств обнаружения и предотвращения вторжений и реализация соответствующих мер;

– эксплуатация средств выявления, анализа уязвимостей ИБ ИСПДн;

– эксплуатация средств защиты сред виртуализации;

– эксплуатация средств защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

– эксплуатация средств межсетевого экранирования;

– эксплуатация и обеспечение наличия средств антивирусной защиты;

– управление конфигурацией СЗПДн;

– осуществление мониторинга СЗПДн;

– формирование предложений по модернизации СЗПДн.

4.9. Менеджеры безопасности ПДн при их обработке в ИСПДн в Обществе назначаются распоряжением Ответственного за организацию обработки ПДн в Обществе.

4.10. Менеджеры безопасности ПДн при их обработке в ИСПДн в Обществе выполняют следующие функции:

– классификация ИС как ИСПДн;

– организация разработки и поддержания в актуальном состоянии карточек процессов обработки ПДн[1];

[1] Порядок формирования и поддержания в актуальном состоянии карточек процессов обработки ПДн приведен в Регламенте обеспечения безопасности ПДн в ПАО «ГМК «Норильский никель», утвержденным в Обществе.

– анализ и систематизация сведений в заполненных карточках процессов обработки ПДн, сведение указанных сведений в перечень процессов обработки ПДн;

– формирование Перечня ПДн на основании сведений, полученных от Менеджеров обработки ПДн в Обществе и Подразделений, обеспечивающих эксплуатацию ИСПДн в Обществе;

– согласование доступа Пользователей ПДн в Обществек ИСПДн;

– формирование Перечня лиц, допущенных к обработке ПДн;

– определение правил и согласование прав доступа к ПДн, обрабатываемых в ИСПДн;

– осуществление методической поддержки работников Общества по вопросам обработки и обеспечения безопасности ПДн;

– формирование рекомендаций по мониторингу СЗПДн и планированию мероприятий по обеспечению безопасности ПДн, в том числе по пересмотру СЗПДн, контроль работ по модернизации СЗПДн;

– участие в установлении необходимого уровня защищенности ПДн при их обработке в ИСПДн;

– организация определения актуальных угроз безопасности ПДн для каждой ИСПДн и разработки моделей угроз безопасности ПДн;

– участие в определении требований по безопасности ПДн при их обработке в ИСПДн;

– проведение мероприятий по внутреннему контролю и (или) аудитов ИБ в части ПДн;

– управление инцидентами ИБ, связанными с обработкой ПДн в ИСПДн.

4.11. Менеджеры обработки ПДн в Обществе назначаются:

– руководителем структурного подразделения, осуществляющего обработку ПДн, по запросу Ответственного за обеспечение безопасности ПДн в Обществе с последующим информированием о произведенных назначениях Ответственного за обеспечение безопасности ПДн в Обществе.

4.12. Менеджеры обработки ПДн в Обществе выполняют следующие функции:

– участие в определении целей и правовых оснований обработки ПДн;

– участие в определении перечня ПДн, обрабатываемых в рамках процессов обработки ПДн в подразделении;

– определение работников структурных подразделений, которым для выполнения трудовых обязанностей необходимо предоставить доступ к ПДн, в том числе в ИСПДн;

– участие в оценке вреда, который может быть причинен субъектам ПДн в случае нарушения требований Федерального закона 152-ФЗ;

– участие в установлении необходимого уровня защищенности ПДн при их обработке в ИСПДн;

– участие в разработке моделей угроз безопасности ПДн в части предоставления необходимых сведений Менеджеру безопасности ПДн при их обработке в ИСПДн в Обществе;

– участие в удалении, уничтожении ПДн, включая уничтожение бумажных носителей ПДн;

– организация заполнения и поддержания в актуальном состоянии карточек процессов обработки ПДн в подразделении;

– выполнение требований РМД Общества в части ПДн;

– участие во взаимодействии с субъектами ПДн, в том числе в подготовке ответа на запросы субъектов ПДн;

– информирование Ответственного за обеспечение безопасности ПДн в Обществе при выявлении фактов несанкционированного доступа в помещения, в которых обрабатываются ПДн;

– поддержка и оказание содействия Ответственному за организацию обработки ПДн в Обществе по его запросу (в том числе при прохождении проверок Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций).

4.13. Работники правовых служб в Обществе выполняют следующие функции:

– совместно с Ответственным за организацию обработки ПДн в Обществе осуществление взаимодействия от имени Общества с Уполномоченным органом по защите прав субъектов ПДн и иными уполномоченными органами в случаях, предусмотренных законодательством РФ в области ПДн;

– осуществление экспертизы РМД Общества и договоров Общества с третьими лицами на предмет их соответствия требованиям законодательства РФ в области ПДн.

4.14. Работники кадровых служб в Обществе выполняют следующие функции:

– организация работы по получению согласий субъектов ПДн на обработку их ПДн;

– информирование Подразделения, организующего опубликование информации об условиях обработки ПДн в Обществе, о необходимости опубликования информации об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц ПДн, разрешенных работником для распространения (информирование производится в срок не позднее 1 (одного) рабочего дня со дня получения от работника согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, содержащего запреты и условия на обработку ПДн неограниченным кругом лиц);

– обработки запросов субъектов ПДн, являющихся работниками Общества, или их представителей и (или) осуществление контроля за приемом и обработкой таких запросов;

– участие в повышении осведомленности по вопросам обработки и обеспечения безопасности ПДн лиц, допущенных к обработке ПДн;

– взаимодействие с работниками Общества по вопросам ознакомления с РМД Общества в области ПДн.

4.15. К Пользователям ПДн в Обществе относятся все работники Общества, участвующие в обработке ПДн и допущенные к обработке ПДн.

4.16. Пользователи ПДн в Обществе выполняют следующие функции:

– участие в определении целей и правовых оснований обработки ПДн;

– обеспечение сохранности носителей ПДн;

– участие в определении перечня ПДн, обрабатываемых в рамках процессов обработки ПДн в подразделении;

– участие в удалении, уничтожении ПДн, включая уничтожение бумажных носителей ПДн;

– участие в разработке и поддержании в актуальном состоянии карточек процессов обработки ПДн;

– выполнение требований РМД Общества в части ПДн;

- участие во взаимодействии с субъектами ПДн;
- контроль точности, полноты и правильности ПДн, вводимых в ИСПДн.

4.17. В Комиссию по обеспечению безопасности ПДн в Обществе включаются следующие участники:

- Ответственный за организацию обработки ПДн в Обществе (председатель Комиссии по обеспечению безопасности ПДн в Обществе);
- Заместитель Генерального директора – начальник отдела ИТ и электронной коммерции Общества;
- Начальник отдела правовой, контрактной работы и закупочной деятельности Общества;
- Главный специалист по персоналу Общества;
- Инженер отдела ИТ и электронной коммерции.

4.18. Дополнительно в Комиссию по обеспечению безопасности ПДн в Обществе могут быть включены работники структурных подразделений Общества, в которых осуществляется обработка ПДн.

4.19. Функции Комиссии по обеспечению безопасности ПДн в Обществе установлены Политикой ООО «Н ТРЭВЕЛ» в области обработки персональных данных.

4.20. Подразделение, организующее опубликование информации об условиях обработки ПДн в Обществе выполняет следующие функции:

- информирование работников кадровых служб Общества о потребности Подразделения, организующего опубликование информации об условиях обработки ПДн в Обществе, в опубликовании ПДн работников на информационных ресурсах Оператора, посредством которых будет осуществляться предоставление доступа к ПДн работника неограниченному кругу лиц (с указанием необходимых ПДн работников, целей опубликования, а также информационных ресурсов Оператора, на которых планируется опубликование ПДн работника), с целью организации получения кадровыми службами Общества согласий работников на обработку ПДн, разрешенных ими для распространения;
- в срок не позднее 2 (двух) рабочих дней с даты получения от Работников кадровых служб в Обществе информации об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц ПДн, разрешенных работником для распространения, организуют опубликование указанной информации на информационных ресурсах Оператора, посредством которых будет осуществляться предоставление доступа к ПДн работника неограниченному кругу лиц.

5. Требования к порядку обработки ПДн

5.1. Обработка ПДн осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом 152-ФЗ и РМД Общества. Обработка ПДн допускается в случаях, установленных частью 1 статьи 6 Федерального закона 152-ФЗ. В Обществе запрашиваются согласия субъекта ПДн на обработку ПДн во всех случаях, когда в соответствии с законодательными требованиями обработка ПДн осуществляется с согласия субъекта ПДн. Формы согласий субъекта ПДн на обработку ПДн (исходя из целей обработки ПДн в Обществе), подлежащие применению в Обществе, а также правила их использования утверждаются распорядительным документом Генерального директора Общества или уполномоченного им лица. Ответственным за разработку и актуализацию форм

согласий субъекта ПДн на обработку ПДн является лицо, ответственное за организацию обработки ПДн.

5.2. Обработка специальных категорий ПДн не допускается, за исключением случаев, если субъект ПДн дал согласие в письменной форме на обработку своих ПДн, и иных случаев, предусмотренных Федеральным законом 152-ФЗ.

5.3. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) и которые используются Обществом для установления личности субъекта ПДн, могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн, за исключением случаев, предусмотренных Федеральным законом 152-ФЗ.

5.4. Общество вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн на основании заключаемого с этим лицом договора (поручения на обработку ПДн).

5.4.1. Обработчик ПДн обязан соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом 152-ФЗ.

5.4.2. В поручении на обработку ПДн должны быть определены:

– Перечень ПДн;

– перечень действий (операций) с ПДн, которые будут совершаться обработчиком ПДн (перечень действий не должен противоречить целям и действиям, заявленным перед субъектом ПДн в договоре, согласии и т. д.);

– цели обработки (цели не должны противоречить целям, заявленным перед субъектом ПДн в договоре, в согласии и т. д.);

– обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке;

– требования к защите ПДн (требования по защите, предъявляемые к лицу, осуществляющему обработку, не должны быть ниже требований, выполняемых самим оператором) и иные сведения в соответствии с законодательством РФ.

5.5. Если ПДн получены Обществом не от субъекта ПДн, Пользователи ПДн в Обществе, за исключением случаев, установленных частью 4 статьи 18 Федерального закона 152-ФЗ, инициируют предоставление субъекту ПДн до начала обработки его ПДн информации, предусмотренной частью 3 статьи 18 Федерального закона 152-ФЗ.

5.6. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки ПДн.

5.6.1. Цели обработки ПДн, действия с ПДн, а также сроки и условия прекращения обработки ПДн определяются в карточке процесса обработки ПДн.

5.6.2. Менеджер обработки ПДн в Обществе и Пользователи ПДн в Обществе должны инициировать заполнение и поддерживать в актуальном состоянии карточки процессов обработки ПДн.

5.6.3. Карточка процесса обработки ПДн (Приложение Г к настоящему Положению) включает в себя:

– цели осуществления обработки ПДн;

– правовые основания обработки ПДн;

– перечень обрабатываемых ПДн;

– перечень лиц и структурных подразделений, осуществляющих обработку ПДн;

- источники получения ПДн;
- перечень действий с ПДн в рамках выполнения процесса;
- особенности неавтоматизированной обработки ПДн;
- особенности автоматизированной обработки;
- сведения об осуществляемой оператором передаче ПДн;
- особенности трансграничной передачи ПДн;
- особенности работы с запросами субъектов ПДн;
- документы, регламентирующие данный процесс обработки ПДн.

5.7. Особенности неавтоматизированной обработки ПДн

5.7.1. Неавтоматизированная обработка ПДн может осуществляться на бумажных носителях информации и/или машинных (съемных) носителях информации (материальные носители ПДн).

5.7.2. При обработке различных категорий ПДн на материальных носителях ПДн необходимо использовать отдельный материальный носитель ПДн для каждой из категорий ПДн.

5.7.3. При обработке ПДн не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

5.7.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес Общества, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых Обществом способов обработки ПДн;

– типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, – при необходимости получения письменного согласия на обработку ПДн;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

– типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

5.7.5. При неавтоматизированной обработке ПДн на бумажных носителях необходимо руководствоваться требованиями Регламента обеспечения безопасности персональных данных в ПАО «ГМК «Норильский никель», утвержденным в Обществе, и требованиями законодательства РФ в части, регламентирующей особенности обработки ПДн, осуществляемой без использования средств автоматизации.

5.7.6. Неавтоматизированная обработка ПДн в электронном виде осуществляется на машинных (съемных) носителях информации.

5.7.7. При необходимости осуществления неавтоматизированной обработки ПДн на машинных (съемных) носителях информации необходимо принимать организационные и технические меры, исключающие возможность несанкционированного доступа к ПДн лиц, не допущенных к их обработке.

5.7.8. Машинные (съемные) носители информации, содержащие ПДн, должны учитываться. Учет машинных (съемных) носителей ПДн осуществляется в соответствии с требованиями Регламента обеспечения безопасности персональных данных ПАО «ГМК «Норильский никель».

5.7.9. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе ПДн, если материальный носитель ПДн не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

– при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе ПДн других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

– при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель ПДн с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

5.7.10. Уточнение ПДн на материальных носителях ПДн производится путем обновления или изменения данных на материальном носителе ПДн, а если это не допускается техническими особенностями материального носителя ПДн, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

5.8. Обработку ПДн могут осуществляться только Пользователи ПДн в Обществе, которым такая обработка необходима в связи с исполнением своих должностных обязанностей (при выполнении условий, предусмотренных в п.10.2, 10.6 настоящего Положения). Процедура предоставления доступа к ИСПДн Пользователей ПДн в Обществе определена НМД в области управления доступом к информационным активам Общества.

5.9. Обработка ПДн допускается только в ИС, для которых установлен уровень защищенности ПДн, обрабатываемых в ИСПДн. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется в соответствии с Регламентом идентификации и классификации информационных активов ПАО «ГМК «Норильский никель» и Регламентом обеспечения безопасности персональных данных в ПАО «ГМК «Норильский никель».

5.10. Общество блокирует обрабатываемые ПДн в следующих случаях:

– выявление неправомерной обработки ПДн при обращении субъекта ПДн или его представителя;

– подтверждение факта неточности ПДн;

– при невозможности уничтожить ПДн в случаях, предусмотренных законодательством РФ в области ПДн;

– по требованию субъекта ПДн или его представителя;

– по требованию Уполномоченного органа по защите прав субъектов ПДн;

– по результатам проведения мероприятий по внутреннему контролю и (или) аудита ИБ;

– в иных предусмотренных законодательством РФ случаях.

6. Особенности передачи ПДн

6.1. Общество в ходе своей деятельности осуществляет передачу ПДн третьим лицам в целях исполнения договорных обязательств, а также с целью обеспечения своей деятельности или исполнения требований законодательства РФ. При этом субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей сведения о лицах (за исключением работников Общества), которые имеют доступ к его ПДн или которым могут быть раскрыты его ПДн на основании договора с Обществом или на основании федерального закона.

6.2. Обществом передаются ПДн только в объеме, необходимом для достижения заявленных целей обработки ПДн.

6.3. Обязательным условием договоров Общества с третьими лицами, в рамках исполнения которых Общество осуществляет передачу (предоставление, доступ) ПДн, является обязанность соблюдения третьими лицами мер обеспечения безопасности ПДн при их обработке. Порядок применения типовых форм разделов в договоры с 3-ми лицами для обеспечения правомерности обмена ПДн приведен в Приложении Д.

6.4. При передаче ПДн работника Общества необходимо:

– не сообщать ПДн работника третьей стороне без письменного согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

– не сообщать ПДн работника в коммерческих целях без его письменного согласия;

– не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

– передавать ПДн работника представителям работников в порядке, установленном Трудовым кодексом и иными федеральными законами, и ограничивать эту информацию только теми ПДн работника, которые необходимы для выполнения указанными представителями их функций;

– предупредить лиц, получающих ПДн работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн работника, обязаны соблюдать режим конфиденциальности.

6.5. Передача ПДн внутри Общества осуществляется только лицам, включенным в Перечень лиц, допущенных к обработке ПДн, и только в необходимом объеме.

6.6. Трансграничная передача ПДн на территории иностранных государств осуществляется в соответствии с Федеральным законом 152-ФЗ.

6.7. В целях информационного обеспечения в Общества создаются общедоступные источники ПДн (в том числе справочники, адресные книги). В общедоступные источники ПДн с письменного согласия субъекта ПДн могут включаться его фамилия, имя, отчество, дата рождения, фотография, должность, подразделение, телефон, адрес электронной почты, табельный номер.

6.8. Особенности обработки ПДн, разрешенных субъектом ПДн для распространения

6.8.1. Передача (распространение) ПДн осуществляется с согласия субъекта ПДн.

6.8.2. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, оформляется отдельно от иных согласий субъекта ПДн на обработку его ПДн. Общество обязано обеспечить субъекту ПДн возможность определить перечень ПДн по каждой категории ПДн, указанной в согласии на обработку ПДн, разрешенных субъектом ПДн для распространения.

6.8.3. В согласии на обработку ПДн, разрешенных субъектом ПДн для распространения, субъект ПДн вправе установить запреты на передачу (кроме предоставления доступа) этих ПДн неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих ПДн неограниченным кругом лиц. Требования к содержанию согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, устанавливаются уполномоченным органом по защите прав субъектов ПДн.

7. Особенности удаления, уничтожения и обезличивания ПДн

7.1. Общество уничтожает ПДн (либо обеспечивает их уничтожение, если обработка ПДн осуществляется другим лицом, действующим по поручению Общества) при прекращении их обработки в случаях:

– достижения целей обработки ПДн (в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн, иным соглашением между Обществом и субъектом ПДн либо если Общество не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом 152-ФЗ или другими федеральными законами;

– невозможности обеспечения правомерности обработки ПДн в случае выявления неправомерной обработки ПДн (в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн) при обращении или по запросу субъекта ПДн (или его представителя) либо Уполномоченного органа по защите прав субъектов ПДн;

– отзыва согласия субъекта ПДн на обработку его ПДн (в случае, если сохранение ПДн более не требуется для целей обработки ПДн) в срок, не превышающий тридцати дней с даты поступления указанного отзыва (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Обществом и субъектом ПДн либо если Общество не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом 152-ФЗ или другими федеральными законами);

– представления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки (в срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки);

– получения соответствующего предписания от Уполномоченного органа по защите прав субъектов ПДн (в соответствии с определенным сроком, не противоречащим законодательству РФ);

– в иных предусмотренных законодательством РФ случаях и в установленные законодательством РФ сроки.

7.2. При невозможности уничтожения ПДн в сроки, определенные абзацами 2-4 п. 7.1 настоящего Положения осуществляется блокирование ПДн и дальнейшее уничтожение ПДн в течение 6 месяцев, если иной срок не установлен законодательством РФ.

7.3. Уничтожение ПДн должно производиться способом, исключающим возможность восстановления этих ПДн. Форма акта об уничтожении ПДн приведена в Приложении Е.

7.4. Обрабатываемые ПДн подлежат удалению из ИСПДн, уничтожению или обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей. Удаление ПДн из ИСПДн осуществляется с помощью штатных средств ИСПДн.

7.5. Уничтожение бумажных носителей ПДн осуществляется в установленном в Обществе порядке после передачи в Архив Общества и (или) истечения сроков хранения.

7.6. Уничтожение ПДн обработчиком ПДн осуществляется в порядке, установленном договором с Обществом.

7.7. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем ПДн, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе ПДн (удаление, вымарывание).

7.8. Требования к методам обезличивания ПДн подразделяются на:

– требования к свойствам обезличенных данных, получаемых при применении метода обезличивания;

– требования к свойствам, которыми должен обладать метод обезличивания.

7.8.1. К требованиям к свойствам получаемых обезличенных данных относятся:

– сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых ПДн);

– сохранение структурированности обезличиваемых ПДн;

– сохранение семантической целостности информации (обезличиваемых ПДн);

– анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания).

7.8.2. К требованиям к свойствам метода обезличивания относятся:

– обратимость (возможность проведения деобезличивания);

– возможность обеспечения заданного уровня анонимности;

– увеличение стойкости при увеличении объема обезличиваемых ПДн.

8. Взаимодействие с субъектами ПДн

8.1. При сборе ПДн необходимо получить согласие субъектов ПДн на обработку ПДн в случаях, предусмотренных законодательством РФ, и по запросу субъектов ПДн необходимо предоставить следующую информацию:

– подтверждение факта обработки ПДн;

– правовые основания и цели обработки ПДн;

– применяемые в Общества способы обработки ПДн;

– наименование и место нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором ПДн (Обществом) или на основании федерального закона;

– обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством РФ;

– сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом 152-ФЗ;

– информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;

– наименование, место нахождения для юридического лица, фамилию, имя, отчество и место жительства для физического лица, осуществляющего обработку ПДн по поручению Общества, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные законодательством РФ.

8.2. От субъектов ПДн или от их уполномоченных представителей могут поступать следующие типы запросов:

– заявление на получение информации, перечисленной в п. 8.1 настоящего Положения;

– заявление на уточнение неполных, неточных или неактуальных ПДн;

– заявление на прекращение обработки ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;

– возражение против решения, принятого на основании исключительно автоматизированной обработки ПДн;

– заявление на отзыв согласия на обработку ПДн;

– заявление на предмет незаконно полученных или избыточных по отношению к заявленной цели обработки ПДн;

– заявление по факту неправомерной обработки ПДн (может быть получено через Уполномоченный орган по защите прав субъектов ПДн).

8.3. Запросы от субъектов ПДн могут поступать в Общество в письменной форме на бумажных или электронных носителях, в том числе по электронной почте. Запрос субъекта ПДн должен содержать необходимые реквизиты и сведения, предусмотренные Федеральным законом 152-ФЗ. К рассмотрению принимаются запросы на бумажным носителях, подписанные собственноручной подписью субъекта ПДн или его законного представителя и запросы в электронном виде, подписанные электронной подписью субъекта ПДн или его законного представителя в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

8.4. Запросы субъектов ПДн в Общество осуществляются при личном посещении субъектом ПДн или направляются в Общество в письменном виде. В случае запроса субъекта ПДн в Общество по телефонной связи Пользователь ПДн в Обществе разъясняет субъекту ПДн, что запрос осуществляется при личном посещении или направляется в Общество в письменном виде.

8.5. Все поступившие запросы субъектов ПДн должны регистрироваться в соответствии с установленным в Обществе правилами делопроизводства.

8.6. Лица, задействованные в подготовке ответа на запросы, должны соблюдать порядок и сроки обработки запросов, установленные законодательством РФ в зависимости от их типов.

9. Взаимодействие с органами государственной власти

9.1. Взаимодействие с органами государственной власти организуется в порядке, установленном действующим законодательством РФ и РМД Общества.

9.2. В случае изменения сведений, указанных в уведомлении об обработке ПДн, Общество направляет информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн, в адрес Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

9.3. Ответственный за организацию обработки ПДн в Обществе устанавливает порядок действий работников Общества при получении информации о предстоящей проверке (в зависимости от вида – плановая или внеплановая), а также при получении запросов от уполномоченных государственных органов.

9.4. Ответственный за организацию обработки ПДн в Обществе осуществляет контроль устранения замечаний, полученных от проверяющих в ходе проведения проверки, до момента ее окончания.

9.5. В случае получения предписания об устранении выявленных нарушений по результатам проведенных проверок Ответственный за организацию обработки осуществляет уведомление Уполномоченного органа по защите прав субъектов ПДн об осуществлении их устранения.

10. Повышение осведомленности Пользователей ПДн в Обществе

10.1. Повышение осведомленности Пользователей ПДн в Обществе в области ИБ осуществляется в соответствии с Регламентом повышения осведомленности работников ПАО «ГМК «Норильский никель» в области информационной безопасности».

10.2. В Обществе к обработке ПДн допускаются только лица, подписавшие обязательство об обеспечении конфиденциальности и безопасности ПДн.

10.3. При трудоустройстве работниками кадровых служб в Обществе осуществляется ознакомление трудоустраиваемых работников с утвержденными РМД Общества, устанавливающими требования и регламентирующими вопросы обработки и обеспечения безопасности ПДн в Общества.

10.4. Инструктаж по вопросам обработки и обеспечения безопасности ПДн проводится в срок не позднее 3-х месяцев со дня приема на работу для вновь трудоустроенных работников, а также в следующих случаях:

- по результатам выявленных нарушений в ходе проведения мероприятий по внутреннему контролю и (или) аудиту ИБ;
- в рамках процесса управления инцидентами ИБ;
- в иных случаях при выявлении соответствующей необходимости.

10.5. Инструктаж по вопросам обработки и обеспечения безопасности ПДн проводится по следующим направлениям:

- требования законодательства РФ в области ПДн;
- правила обработки ПДн в Общества;

– общие вопросы обеспечения ИБ в Общества;

– ответственность за нарушение правил обработки и обеспечения безопасности ПДн.

10.6. Пользователи ПДн в Обществе допускаются к обработке ПДн только после:

– ознакомления с требованиями настоящего Положения, Политики Общества в области обработки персональных данных, иных РМД Общества, регулирующих обработку ПДн в Обществе и устанавливающих ответственность за нарушение установленных в Обществе правил обработки и обеспечения безопасности ПДн, выполнение которых обязательно для соответствующих работников;

– прохождения инструктажа по правилам обработки и обеспечения безопасности ПДн (при наличии автоматизированной системы повышения осведомленности работников по вопросам ИБ инструктаж может проводится дистанционно);

– включения Пользователя ПДн в Перечень лиц, допущенных к обработке ПДн.

11. Обеспечение безопасности ПДн

11.1. Для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн применяется комплекс организационных, технических и организационно–технических мер ИБ, в совокупности составляющих СЗПДн. Требования к составу мер ИБ и порядку их выполнения устанавливаются Регламентом обеспечения безопасности персональных данных в ПАО ГМК «Норильский никель» и Стандартом обеспечения информационной безопасности на стадиях жизненного цикла информационных систем и автоматизированных систем управления технологическими процессами ПАО «ГМК «Норильский никель».

11.2. Для каждой ИСПДн должно быть определено физическое или юридическое лицо, являющееся оператором ИСПДн. В случае поручения обработки ПДн безопасность ПДн обеспечивает обработчик ПДн в соответствии с законодательством РФ.

11.3. Определение оператора ИСПДн осуществляется следующим способом:

– если программно-техническая база ИСПДн принадлежат одному юридическому лицу, при этом это юридическое лицо не имеет договора, в котором оно поручало бы эксплуатацию данной ИСПДн другому юридическому лицу, то оно является оператором данной ИСПДн;

– если юридическое лицо осуществляет эксплуатацию ИСПДн в соответствии с договором, заключенным с юридическим лицом, являющимся владельцем программно-технической базы ИСПДн, то оно является оператором данной ИСПДн;

– если программно-техническая база ИСПДн принадлежит разным юридическим лицам, между этими юридическими лицами должен быть заключен договор, по которому одно из этих юридических лиц осуществляет эксплуатацию ИСПДн. Юридическое лицо, осуществляющее эксплуатацию ИСПДн, и будет являться оператором данной ИСПДн.

11.4. Меры по обеспечению безопасности ПДн при их обработке, осуществляемой без использования средств автоматизации:

– обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей ПДн) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;

– необходимо обеспечивать раздельное хранение ПДн (материальных носителей ПДн), обработка которых осуществляется в различных целях;

– при хранении материальных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

11.4.1. Порядок доступа работников в помещения, в которых ведется обработка ПДн, устанавливается РМД Общества, регламентирующими процессы обеспечения физической защиты объектов.

11.4.2. Обеспечение безопасности ПДн от уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн достигается, в том числе, установлением правил доступа в помещения, в которых ведется обработка ПДн, как с использованием средств автоматизации, так и без использования средств автоматизации.

11.4.3. Размещение ИСПДн осуществляется в охраняемых помещениях. Для помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей ПДн и СЗИ, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

11.4.4. В целях соблюдения требований к ограничению доступа в помещения, в которых ведется обработка ПДн, должно быть обеспечено:

– использование помещений строго по назначению;

– наличие на входах в помещения дверей, оборудованных запорными устройствами;

– содержание дверей помещений в нерабочее время в состоянии, закрытом на запорное устройство;

– содержание окон в помещениях в нерабочее время в закрытом состоянии.

11.4.5. При хранении материальных носителей ПДн в помещениях должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним.

11.4.6. Нахождения лиц, не уполномоченных осуществлять обработку ПДн, в помещениях возможно только в сопровождении работников вышеуказанных структурных подразделений или должностных лиц Общества на время, ограниченное служебной необходимостью.

11.4.7. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения третьих лиц, о случившемся должно быть немедленно сообщено лицу, ответственному за организацию доступа в помещение.

12. Проведения оценки вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона 152-ФЗ

12.1. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Обществом требований Федерального закона 152-ФЗ, осуществляется Комиссией по обеспечению безопасности ПДн в Общества.

12.2. Согласно части 2 статьи 17 Федерального закона 152-ФЗ вред субъекту ПДн может быть причинен в следующих формах:

– убытки[2] – расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода);

– моральный вред[3] – физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

12.3. В зависимости от значительности последствий для субъекта ПДн в случае нарушения Федерального закона 152-ФЗ Комиссией по обеспечению безопасности ПДн в Общества устанавливается один из следующих уровней вреда субъектам ПДн – низкий, средний, высокий.

12.4. Оценка вреда субъектам ПДн определяется экспертно, с использованием информации о категории ПДн, объеме ПДн, обрабатываемых Обществом, и категорий субъектов ПДн.

13. Контроль за соблюдением требований в области обработки и защиты ПДн

13.1. В целях соблюдения обязательных требований в области обработки и обеспечения безопасности ПДн в Общества Ответственным за обеспечение безопасности ПДн в Обществе и Менеджером безопасности ПДн при их обработке в ИСПДн в Обществе регулярно проводятся следующие мероприятия по внутреннему контролю и (или) аудиты ИБ в части ПДн:

– соответствия процессов обработки ПДн в структурных подразделениях Общества требованиям законодательства РФ и РМД Общества в области ПДн;

– актуальности и соответствия законодательству РФ, имеющихся РМД Общества в области обработки ПДн;

– актуальности Перечня ПДн;

– актуальности Перечня лиц, допущенных к обработке ПДн;

– актуальности перечня ИСПДн;

– актуальности перечня структурных подразделений, участвующих в обработке ПДн в Общества;

– актуальности прав разграничения доступа Пользователей ПДн в Обществе к ИСПДн, необходимых для выполнения должностных обязанностей;

– актуальности предоставленной в Уполномоченный орган по защите прав субъектов ПДн информации об обработке ПДн;

– знания работниками законодательства РФ в области ПДн, порядка обработки ПДн и поддержания порядка обеспечения безопасности ПДн;

[2] Часть 2 статьи 15 Гражданского кодекса Российской Федерации.

[3] Статья 151 Гражданского кодекса Российской Федерации.

- состояния мер обеспечения безопасности ПДн;
- состояния мер по соблюдению прав субъектов ПДн.

13.2. При проведении мероприятий по внутреннему контролю и (или) аудитов ИБ в части ПДн применяются требования (контроли) действующего законодательства РФ в области ПДн.

13.3. Ответственный за организацию обработки ПДн в Общества ежегодно утверждает программу проведения мероприятий по внутреннему контролю и (или) аудитов ИБ (далее - программа аудита ИБ) в части ПДн. Ответственный за обеспечение безопасности ПДн в ГО Общества формирует предложения в отношении программы аудита ИБ и осуществляет подготовку ее проекта.

13.4. Программа аудита ИБ в части ПДн должна включать в себя информацию и ресурсы, необходимые для организации мероприятий по внутреннему контролю и (или) аудитов ИБ в части ПДн и их результативного и эффективного проведения в установленные временные сроки, а также может включать в себя следующее:

- цели для программы аудита ИБ;
- объем/количество/типы/места проведения и график проведения мероприятий по внутреннему контролю и (или) аудитов ИБ;
- процедуры программы аудита ИБ;
- критерии внутреннего контроля и (или) аудита ИБ;
- методы внутреннего контроля и (или) аудита ИБ;
- формирование группы (групп) по внутреннему контролю и (или) аудиту ИБ;
- необходимые ресурсы, включая расходы на командировки и размещение Менеджеров безопасности ПДн при их обработке в ИСПДн Общества.

13.5. Планы мероприятий по внутреннему контролю и (или) аудитов ИБ в части ПДн разрабатываются с учетом статуса и важности проверяемых процессов, подлежащих контролю, а также результатов предыдущих мероприятий по внутреннему контролю и (или) аудитов ИБ в части ПДн.

13.6. План мероприятий по внутреннему контролю и (или) аудита ИБ в части ПДн должен включать в себя:

- цели мероприятий по внутреннему контролю и (или) аудита ИБ;
- область мероприятий по внутреннему контролю и (или) аудита ИБ, включая идентификацию организационных и функциональных подразделений и процессов, которые будут проверяться;
- критерии внутреннего контроля и (или) аудита ИБ и ссылочные документы;
- места проведения мероприятий по внутреннему контролю и (или) аудита ИБ, даты, ожидаемое время и продолжительность намеченных мероприятий по внутреннему контролю и (или) аудиту ИБ, включая совещания с руководством Общества, а также другие совещания;
- используемые при проведении мероприятий по внутреннему контролю и (или) аудита ИБ методы, включая объем или степень выборочного контроля, необходимого для получения достаточных свидетельств внутреннего контроля и (или) аудита ИБ;
- роли и обязанности членов группы по внутреннему контролю и (или) аудиту ИБ, а также сопровождающих лиц и наблюдателей;
- распределение соответствующих ресурсов;

– период проведения мероприятий по внутреннему контролю и (или) аудита ИБ.

13.7. По результатам проведения каждого мероприятия по внутреннему контролю и (или) аудита ИБ в части ПДн Менеджером безопасности ПДн при их обработке в ИСПДн в Обществе составляется отчет.

13.8. Отчет по результатам проведения мероприятий по внутреннему контролю и (или) аудита ИБ в части ПДн должен включать в себя:

– цель мероприятий по внутреннему контролю и (или) аудита ИБ;

– область проведения мероприятий по внутреннему контролю и (или) аудита ИБ;

– общая информация об объекте внутреннего контроля и (или) аудита ИБ;

– оценка соответствия критериям внутреннего контроля и (или) аудита ИБ;

– выявленные недостатки;

– рекомендации по модернизации организационных и технических мер по обеспечению безопасности ПДн;

– описание процессов обработки ПДн;

– описание ИТ-инфраструктуры;

– описание ИСПДн;

– описание применяемых организационных и технических мер по обеспечению безопасности ПДн.

13.9. В случае получения информации о факте нарушения действующего законодательства РФ и РМД Общества в области ПДн Ответственный за организацию обработки ПДн в Общества инициирует проверку инцидента ИБ в соответствии с Регламентом управления инцидентами информационной безопасности в ПАО «ГМК «Норильский никель» для выявления лиц, в результате действий или бездействия которых произошло нарушение.

13.10. Менеджер обработки ПДн в Обществе, ответственный за область проведения мероприятий по внутреннему контролю и (или) аудита ИБ, должен своевременно и без задержки обеспечить проведение проверки устранения обнаруженных несоответствий и их причин. Последующие действия должны включать в себя проверку предпринятых действий и сообщение о результатах проверки.

14. Ответственность

14.1. Ответственность за ненадлежащую организацию и неосуществление контроля исполнения требований настоящего Положения, а также за несвоевременное внесение изменений и дополнений в настоящее Положение несет лицо ответственное за организацию обработки ПДн.

14.2. Все участники процессов обработки и обеспечения безопасности ПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных Положением.

Приложение А

Нормативные ссылки

При разработке Положения были использованы следующие нормативные документы:

от 30.12.2001 № 197-ФЗ	Трудовой кодекс Российской Федерации
от 30.11.1994 № 51-ФЗ	Гражданский кодекс Российской Федерации. Часть первая
от 27.07.2006 № 149-ФЗ	Федеральный закон «Об информации, информационных технологиях и о защите информации»
от 27.07.2006 № 152-ФЗ	Федеральный закон «О персональных данных»
от 06.04.2011 № 63-ФЗ	Федеральный закон «Об электронной подписи»
от 15.09.2008 № 687	Постановление Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
от 01.11.2012 № 1119	Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
от 24.02.2021 № 18	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»
ГОСТ Р ИСО/МЭК 27001-2021	Национальный стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
_____	Политика ООО «Н ТРЭВЕЛ» в области обработки персональных данных
С ГК НН 167-001-2020	Стандарт обеспечения информационной безопасности на стадиях жизненного цикла информационных систем и автоматизированных систем управления технологическими процессами ПАО «ГМК «Норильский никель»
Р ГК НН 167-005-2020	Регламент обеспечения безопасности персональных данных в ПАО «ГМК «Норильский никель»
Р ГК НН 167-003-2019	Регламент управления инцидентами информационной безопасности в ПАО «ГМК «Норильский никель»

Р ГК НН 167-007-2019	Регламент идентификации и классификации информационных активов ПАО «ГМК «Норильский никель»
Р ГК НН 167-003-2020	Регламент повышения осведомленности работников ПАО «ГМК «Норильский никель» в области информационной безопасности

Приложение Б

Сокращения и аббревиатуры

ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
ИСПДн	Информационная система персональных данных
Кадровая служба	Структурное подразделение Общества или организации, оказывающей услуги в области кадрового администрирования (в рамках заключенного договора)
Карточка процесса обработки ПДн	Структурированная информация о целях осуществления обработки ПДн; правовых основаниях обработки ПДн; перечне обрабатываемых ПДн; перечне категорий лиц и структурных подразделений, осуществляющих обработку ПДн; источниках получения ПДн; перечне действий с ПДн в рамках выполнения процесса; об особенностях неавтоматизированной и автоматизированной обработки ПДн; о передаче ПДн; об особенностях трансграничной передачи ПДн; об особенностях работы с обращениями субъектов ПДн
Общество	ООО «Н ТРЭВЕЛ»
Менеджер безопасности ПДн при их обработке в ИСПДн в Обществе	Работник Службы ИБ Общества, ответственный за определение мероприятий по обеспечению безопасности ПДн
Менеджер обработки ПДн в Обществе	Работники подразделений Общества, в которых обрабатываются ПДн, ответственные за предоставление сведений об обрабатываемых ПДн в ИСПДн, заполнение и актуализацию карточек процессов обработки ПДн
Обязательство об обеспечении конфиденциальности и безопасности ПДн	Обязательство лица, получившего доступ к персональным данным, обеспечивать конфиденциальность и безопасность персональных данных, в том числе: не разглашать персональные данные; не передавать без служебной необходимости третьим лицам и не раскрывать публично персональные данные; информировать

	непосредственного руководителя об утрате носителей персональных данных и иных инцидентах информационной безопасности, связанных с персональными данными.
Паспорт ИС	Структурированная информация о назначении ИС, владельце ИС, расположении ИС, классификации ИС, перечне обрабатываемой в ИС информации, перечне основных технических средств, перечне программным продуктов, перечне документации на ИС, сетевых сервисах, схемах сетевой инфраструктуры ИС, перечне привилегированных учетных записях
ПДн	Персональные данные
Перечень лиц, допущенных к обработке ПДн	Перечень лиц, доступ которых к ПДн, обрабатываемым в информационных системах персональных данных (ИСПДн), необходим для выполнения ими трудовых обязанностей, а также лиц, осуществляющих неавтоматизированную обработку ПДн
Перечень ПДн	Перечень подлежащих обработке ПДн
ПО	Программное обеспечение
Подразделение, организующее опубликование информации об условиях обработки ПДн в Обществе	Структурное подразделение Общества, на которое в установленном порядке возложены функции по организации опубликования информации об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц ПДн, разрешенных работником для распространения на информационных ресурсах Оператора (в рамках исполнения обязанности, возложенной на Оператора ч.10 ст.10.1 Федерального закона 152-ФЗ)
Пользователь ПДн	Работник Общества, осуществляющий обработку ПДн в рамках исполнения трудовых обязанностей
РМД	Регламентирующие документы (нормативно-методические/организационно-правовые документы)
РФ	Российская Федерация
СЗИ	Средства защиты информации
СЗПДн	Система защиты персональных данных

Федеральный закон 152-ФЗ	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
УЗ	Уровень защищенности ПДн, обрабатываемых в ИСПДн
Уполномоченный орган по защите прав субъектов ПДн	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
RPO	Целевая точка восстановления (Recovery Point Objective)
RTO	Целевое время восстановления (Recovery Time Objective)

Приложение В

Термины

Термины представлены в отдельном файле в формате Excel, являющемся неотъемлемой частью данного Положения.

Глоссарий.xlsx

Приложение Г

Шаблон карточки процесса обработки ПДн

Карточка процесса обработки ПДн

«*Наименование процесса обработки ПДн*»

История исправлений

Дата	Версия	Автор	Подпись	Комментарий

1. Общие сведения

1.1. Менеджер обработки ПДн

1.2. Цели осуществления обработки ПДн

1.3. Правовые основания обработки ПДн

1.4. Перечень обрабатываемых ПДн

№ п\п	Категории субъектов ПДн	Состав обрабатываемых ПДн

1.5. Пользователи ПДн

№	Структурное подразделение	Должность	ФИО	Допуск к обработке ПДн				Неавтоматизированная обработка (осуществляется/не осуществляется)	Автоматизированная обработка	
				Права доступа к ПДн (чтение, добавление, удаление, изменение, передача)	Категории субъектов ПДн	Состав обрабатываемых ПДн	Категория ПДн		ИСПДн	Полномочия в ИСПДн

2. Описание процесса обработки ПДн

2.1. Источники получения ПДн

2.2. Перечень действий с ПДн в рамках выполнения процесса

Сбор		Запись		Систематизация	
Накопление		Хранение		Уточнение (обновление, изменение)	
Извлечение		Использование		Передача (распространение)	
Передача (предоставление)		Передача (доступ)		Обезличивание	
Блокирование		Удаление		Уничтожение	

2.3. Особенности неавтоматизированной обработки ПДн

- Форма и место хранения материальных носителей ПДн

№ п\п	Носители персональных данных	Места хранения (адрес, № помещения, сейфа, шкафа)	Категория ПДн	Срок хранения	Порядок уничтожения, номер документа об уничтожении (акта, приказа)	Ответственный за хранение

2.4. Особенности автоматизированной обработки

- Перечень ИСПДн

№ п\п	Наименование	Категория ПДн	Объем ПДн	Субъекты ПДн	УЗ

- Сроки хранения ПДн
- Порядок удаления, уничтожения или обезличивания ПДн

2.5. Сведения об осуществляемой оператором передаче ПДн

2.6. Особенности трансграничной передачи ПДн

2.7. Особенности работы с запросами субъектов ПДн

- Место хранения журнала учета запросов субъектов ПДн
- Описание порядка работы с запросами субъектов ПДн

2.8. Документы, регламентирующие данный процесс обработки ПДн

Приложение Д

Инструкция по применению разделов для договоров с 3-ми лицами – раздела о поручении обработки персональных данных и раздела о защите персональных данных

1. Для обеспечения выполнения требований законодательства РФ в сфере ПДн при организации обмена ПДн с 3-ми лицами (контрагентами) в случаях, указанных в п.п. 1.1-1.3 настоящей Инструкции, следует включать в договоры с данными лицами следующие типовые разделы:

(1) раздел о защите ПДн;

(2) раздел о поручении обработки ПДн.

1.1. Необходимость в заключении договора, содержащего раздел о защите ПДн, возникает в том случае, если:

(1) передача ПДн не является самостоятельным предметом правоотношений (договора) между сторонами и носит вспомогательный (обеспечивающий) характер по отношению к основному предмету таких отношений;

(2) все возможное многообразие действий по обработке ПДн ограничено только передачей ПДн между сторонами.

1.2. Необходимость в заключении договора, содержащего раздел о поручении обработки ПДн, возникает в том случае, если:

(1) обработка ПДн является самостоятельным предметом правоотношений (договора) между оператором и лицом, осуществляющим обработку ПДн по поручению оператора;

(2) возмездное выполнение лицом-«обработчиком» различных действий с ПДн неразрывно связано с достижением цели обработки ПДн, определенной оператором.

1.3. Раздел о защите ПДн входит в состав Общих условий договоров, размещенных на официальном сайте ПАО «ГМК «Норильский Никель», и **его следует включать во все договоры с контрагентами.**

Раздел о поручении обработки ПДн следует включать в договоры с контрагентами в отдельных случаях, соответствующих условиям из п.1.2 настоящей Инструкции (примеры приведены в таблице ниже).

1.4. В таблице ниже приведено сравнение вышеупомянутых разделов для договоров с 3-ми лицами, включая примеры ситуаций для применения каждого раздела.

Раздел о поручении обработки ПДн	**Раздел о защите ПДн**
Предмет	
Предметом раздела (соглашения) о поручении обработки ПДн является	Предметом раздела (соглашения) о защите ПДн является

Раздел о поручении обработки ПДн	**Раздел о защите ПДн**
осуществление обработки ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.	обеспечение правомерности передачи (предоставления, доступа) ПДн между сторонами соглашения, а также обеспечение конфиденциальности и безопасности передаваемых между сторонами соглашения ПДн при их обработке.
Стороны	
Сторонами договора, содержащего раздел о поручении обработки ПДн являются: 1. оператор; 2. лицо, осуществляющее обработку ПДн по поручению оператора.	Сторонами договора, содержащего раздел о защите ПДн являются: 1. передающая сторона; 2. получающая сторона.
Применимые ситуации	
Раздел о поручении обработки ПДн следует рассматривать как приоритетный механизм формализации правоотношений при обмене ПДн в ситуации передачи оператором специализированному поставщику определённых бизнес-процессов (аутсорсинг бизнес-процессов). Стоит отметить, что в этой ситуации оператор сохраняет значительную степень контроля над формой и содержанием переданного бизнес-процесса. Оператор **определяет** результат обработки ПДн, осуществляемой поставщиком с целью реализации переданного ему на аутсорсинг бизнес-процесса. **Перечень примеров** (не является исчерпывающим) вышеперечисленных ситуаций:	Раздел о защите ПДн следует рассматривать как приоритетный механизм формализации правоотношений при обмене ПДн в ситуации передачи оператором поставщику только определенных функций или элементов бизнес-процессов (аутсорсинг отдельных задач). Стоит отметить, что оператор не осуществляет контроль над деятельностью своих поставщиков, контролируя лишь соблюдение указанных в договоре требований к полноте, качеству, срокам результата деятельности поставщиков. Оператор **не определяет** результат обработки ПДн, осуществляемой поставщиком, а требует от последнего только ранее оговоренный в договоре результат оказания услуг или выполнения работ.

Раздел о поручении обработки ПДн	Раздел о защите ПДн
1. ведение преддоговорной деятельности, оказание услуг, выполнение работ или поставка товаров посредством лиц, с которыми заключаются агентские договоры; 2. обеспечение безопасности на объектах недвижимости (услуги в сфере охраны), связанное с осуществлением учета посетителей и (или) видеонаблюдения; 3. работа с обращениями и запросами от заинтересованных лиц (услуги центра обработки вызовов, опросы/анкетирование для мероприятий); 4. организация и управление деловыми поездками работников (услуги бизнес-туризма); 5. организация визово-миграционной поддержки; 6. архивирование, хранение и уничтожение материальных носителей с ПДн (архивные услуги); 7. предоставление комплексных ИТ-услуг (провайдер услуг является оператором тех ИС, которые используются заказчиком); 8. кадровое, бухгалтерское и ИТ сопровождение; 9. внешний подбор персонала (кадровые агентства, сервисы), осуществляемый на основании агентских договоров;	**Перечень примеров** (не является исчерпывающим) вышеперечисленных ситуаций: 1. оказание услуг, выполнение работ или поставка товаров в пользу субъекта ПДн, являющегося стороной договора или выгодоприобретателем по нему; 2. банковские зарплатные проекты; 3. страхование (имущественное и личное); 4. бронирование и приобретение гостиничных мест и транспортных билетов, услуги такси; 5. выполнение переводов текстов с одного языка на другой; 6. совершение нотариальных действий; 7. внешний подбор персонала (кадровые агентства, сервисы), осуществляемый на основании договоров оказания услуг; 8. услуги связи (операторы связи); 9. использование инфраструктуры электронного документооборота (сдача обязательной отчетности в ОГВ, взаимодействие с партнерами и т.п.); 10. внешнее обучение и аттестация (заказчик не диктует исполнителю содержание и форму обучения/аттестации); 11. медицинские осмотры и освидетельствования; 12. внешний финансовый аудит и контроль; 13. изготовление полиграфической продукции (визитки, корпоративные издания и плакаты);

Раздел о поручении обработки ПДн	Раздел о защите ПДн
	14. справочно-информационные сервисы (СПАРК, Интегрум, Кронос-Информ); 15. посреднические услуги (визовые центры); 16. предоставление ИТ-инфраструктуры, колокация, техническое обслуживание ИС (провайдер услуг не берет на себя роль оператора ИС заказчика).

Типовая форма раздела по защите ПДн для договора

Раздел 1. Защита персональных данных

1.1. Стороны в соответствии с требованиями части 1 статьи 6 и части 4 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» обязуются проявлять должную осмотрительность и обеспечивать правомерную передачу персональных данных друг другу в составе и сочетании, необходимом для достижения одной, нескольких или всех нижеперечисленных целей, актуальных для взаимоотношений между Сторонами:

- заключение и (или) исполнение договоров и соглашений между Сторонами;
- установление и поддержание делового общения между Сторонами;
- осуществление информационного взаимодействия между Сторонами;
- осуществление прав, исполнение обязанностей и соблюдение запретов, предусмотренных применимым к деятельности Сторон законодательством.

1.2. Каждая из Сторон является самостоятельно действующим оператором в отношении передаваемых ей другой Стороной персональных данных. Иное должно быть прямо указано в соглашении о поручении обработки персональных данных, если такое соглашение будет заключено между Сторонами в отношении отдельных случаев обработки персональных данных.

1.3. На основании соответствующего запроса, поступившего от получающей Стороны, передающая Сторона в разумный срок, но не позднее 5 (пяти) рабочих дней с даты получения запроса, предоставляет получающей Стороне подтверждение либо факта получения согласия субъектов на осуществление передачи их персональных данных, либо наличия иных правовых оснований для осуществления передачи персональных данных субъектов и подтверждение факта надлежащего уведомления субъектов о передаче их персональных данных.

1.4. Стороны обязуются обеспечивать конфиденциальность и безопасность передаваемых друг другу персональных данных при их обработке

в соответствии с требованиями статьи 7 и части 1 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.5. В предусмотренных договором целях получающая Сторона имеет право привлекать третьих лиц к обработке персональных данных, полученных от передающей Стороны, путем поручения третьим лицам обработки указанных персональных данных и (или) путем передачи третьим лицам персональных данных без поручения обработки персональных данных. Привлечение третьих лиц к обработке персональных данных может осуществляться только при наличии соответствующих правовых оснований у получающей Стороны и при условии обеспечения третьими лицами конфиденциальности и безопасности персональных данных при их обработке. Если получающей стороной является ПАО «ГМК «Норильский никель» или организация, входящая в его группу лиц, то под третьими лицами понимается любая организация, входящая в группу лиц ПАО «ГМК «Норильский никель».

1.6. Сторона обязуется возместить другой Стороне убытки в размере причиненного и документально подтвержденного реального ущерба, причиненного потерпевшей Стороне вследствие осуществления Стороной неправомерной передачи персональных данных в адрес потерпевшей Стороны, а также при нарушении Стороной конфиденциальности и (или) безопасности при обработке передаваемых ей потерпевшей Стороной персональных данных.

1.7. Положения настоящего раздела действуют в течение срока действия договора, а также сохраняют свое действие после его прекращения в рамках законодательно установленных требований по организации обработки и защиты персональных данных.

1.8. Если иное не предусмотрено договором, все уведомления и сообщения, направляемые Сторонами друг другу в соответствии с настоящим разделом или в связи с ним, должны быть переданы по электронной почте по адресам, указанным в разделе договора о реквизитах Сторон.

Типовая форма раздела поручения на обработку ПДн для договора

2. Поручение на обработку персональных данных

2.1. Заказчик (Оператор) на основании и во исполнение Договора поручает Исполнителю (Обработчику) для достижения следующих целей: _____ *(указать цели обработки)* обработку персональных данных в следующем составе: _____ *(указать перечень ПДн)*.

2.2. Оператор гарантирует Обработчику наличие согласия субъектов персональных данных в отношении данного поручения.

2.3. Обработчик вправе осуществлять с персональными данными такие действия как уточнение (обновление, изменение), передача (распространение, предоставление, доступ), блокирование, удаление, уничтожение, _____ *(при необходимости дополнить: сбор, запись, систематизация, накопление, хранение, извлечение, использование, обезличивание)*с использованием средств автоматизации и без использования средств автоматизации.

2.4. Обработчик обязан принимать необходимые меры обеспечения конфиденциальности (в том числе в соответствии с частью 5 статьи 18 и статьей 18.1 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных») и безопасности (в том числе в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных») или обеспечивать их принятие при обработке персональных данных с использованием средств автоматизации и (или) без использования средств автоматизации в соответствии с требованиями применимого законодательства, предъявляемыми к защите персональных данных, в том числе для поддержания соответствующего уровня защищенности персональных данных при их обработке в информационных системах, в зависимости от типа актуальных угроз безопасности персональных данных.

2.5. В зависимости от способа обработки персональных данных обеспечение Обработчиком безопасности персональных данных достигается:

- определением угроз безопасности персональных данных, которые могут возникнуть при их обработке в информационных системах Обработчика;
- применением организационных и (или) технических мер по обеспечению безопасности персональных данных при их обработке, в том числе в информационных системах Обработчика, необходимых для обеспечения постоянной конфиденциальности, целостности, доступности и устойчивости процессов и (или) систем, связанных с обработкой персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах Обработчика;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы Обработчика;
- определением мест хранения материальных носителей персональных данных, а также обеспечением учета и сохранности материальных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием надлежащих мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы Обработчика, связанные с обработкой персональных данных, и по реагированию на компьютерные инциденты в них;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем Обработчика, связанных с обработкой персональных данных;
- установлением перечня лиц, привлеченных к обработке персональных данных, в том числе в информационных системах Обработчика, и ограничением доступа к персональным данным для иных лиц;

- организацией режима безопасности помещений, в которых осуществляется обработка персональных данных и (или) размещены программно-аппаратные средства, используемые для обработки персональных данных;
- установлением правил доступа к персональным данным, обрабатываемым в информационных системах Обработчика, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах Обработчика;
- назначением лица, ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах Обработчика.

2.6. По требованию Оператора Обработчик обязуется предоставлять документы и иную информацию, подтверждающие принятие Обработчиком вышеуказанных мер обеспечения конфиденциальности и безопасности персональных данных в целях исполнения поручения Оператора, а также по требованию Оператора, но не чаще чем один раз в год, предоставлять ему возможность проведения проверки состояния безопасности обрабатываемых в рамках данного поручения персональных данных и принимаемых Обработчиком мер по обеспечению безопасности персональных данных, а также оказывать содействие и не препятствовать при проведении проверки.

2.7. Обработчик обязуется осуществить обработку персональных данных в рамках данного поручения лично либо по согласованию с Оператором и на условиях, предусмотренных данным поручением, привлечь к обработке (перепоручить обработку) персональных данных третьих лиц, оставаясь ответственным перед Оператором за выполнение своих обязательств по данному поручению.

2.8. В случае, если Обработчику поручается обработка персональных данных без использования средств автоматизации, Обработчик обязуется своевременно проинформировать лиц, допущенных Обработчиком к обработке персональных данных без использования средств автоматизации в рамках данного поручения, о факте обработки указанными лицами персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных применимыми нормативными правовыми актами, включая Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. Постановлением Правительства РФ от 15.09.2008 № 687). Обработчик обязуется в течение 7 (семи) дней с даты получения требования Оператора предоставить сведения и документы, подтверждающие факт надлежащего исполнения Обработчиком обязанности, предусмотренной настоящим пунктом.

2.9. В случае, если Обработчику поручается обработка персональных данных с использованием средств автоматизации, Обработчик обязуется осуществлять или обеспечить осуществление сбора и последующей обработки (запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение) персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

2.10. Стороны обязуются в течение 3 (трех) дней уведомлять друг друга о следующих событиях:

- получение Стороной запроса, претензии, иска или требования от субъекта (представителя субъекта) персональных данных, уполномоченного органа или иного лица по предполагаемому неисполнению или ненадлежащему исполнению Оператором обязанности иметь согласие субъекта персональных данных;
- получение Стороной запроса субъекта (представителя субъекта) персональных данных на доступ, уточнение, блокирование или уничтожение его персональных данных, обрабатываемых Обработчиком в рамках данного поручения;
- получение Стороной запроса уполномоченного органа в отношении надлежащей организации обработки и обеспечения безопасности персональных данных, обрабатываемых Обработчиком в рамках данного поручения;
- обнаружение факта нарушения или подозрение о нарушении конфиденциальности и безопасности обработки персональных данных, обрабатываемых Обработчиком в рамках данного поручения.

2.11. Обработчик обязуется в течение 3 (трех) дней с момента получения требования Оператора в отношении определенных в этом требовании персональных данных, обрабатываемых Обработчиком в рамках данного поручения, проводить их уточнение (обновление, изменение), передачу (предоставление, доступ), блокирование, удаление, уничтожение.

2.12. Настоящим Стороны соглашаются добросовестно сотрудничать и оказывать необходимое содействие друг другу при урегулировании с субъектами персональных данных, уполномоченными органами государственной власти и иными лицами запросов, претензий, исков или требований, полученных Оператором и (или) Обработчиком в отношении настоящего поручения.

2.13. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Обработчик обязан с момента выявления такого инцидента (в том числе уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом) уведомить Оператора:

- в течение двенадцати часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Обработчиком на взаимодействие с Оператором и уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
- в течение сорока восьми часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

2.14. Обработчик обязуется возместить Оператору убытки в размере причиненного и документально подтвержденного реального ущерба, причиненного Оператору вследствие несоблюдения Обработчиком цели и состава действий по обработке персональных данных, указанных в данном поручении, или нарушения Обработчиком конфиденциальности и (или) безопасности персональных данных, обрабатываемых Обработчиком в рамках данного поручения.

2.15. Положения настоящего раздела действуют в течение всего срока действия Договора. С даты прекращения действия Договора Обработчик прекращает обработку персональных данных и возвращает Оператору все персональные данные или, при наличии указания Оператора, уничтожает все персональные данные с письменным подтверждением такого уничтожения, если иное не установлено действующим законодательством.

2.16. Все уведомления и сообщения, направляемые Сторонами друг другу в соответствии с настоящим разделом или в связи с ним, должны быть переданы по электронной почте по адресам [, указанным в разделе Договора о реквизитах Сторон] / [Заказчика: _____, Исполнителя: _____].

Приложение Е

Форма акта об уничтожении персональных данных

АКТ N _
об уничтожении (о прекращении обработки)
персональных данных

г. _____ «____» _____ 2023 г.

Комиссия в составе:

(1) [*Фамилия Имя Отчество*], [*Наименование должности*] – председатель комиссии;

(2) [*Фамилия Имя Отчество*], [*Наименование должности*] – член комиссии;

(3) [*Фамилия Имя Отчество*], [*Наименование должности*] – член комиссии,

руководствуясь Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных», составила настоящий акт о том, что ООО «Н ТРЭВЕЛ» произведено уничтожение персональных данных:

Дата уничтожения	
Наименование Оператора ПДн[1]	
ФИО субъектов/иная информация[2], относящаяся к лицам, чьи ПДн были уничтожены	
Перечень категорий уничтоженных ПДн[3]	
Наименование уничтоженных материальных носителей, содержащих ПДн, с указанием количества листов в отношении каждого материального носителя (в случае неавтоматизированной обработки ПДн);	
Наименование ИСПДн, из которой были уничтожены ПДн (в случае автоматизированной обработки ПДн);	
Способ уничтожения ПДн	
Причина уничтожения	

Председатель комиссии: _____/ _____ /
(подпись) (расшифровка подписи)

Члены комиссии: _____/ _____ /
(подпись) (расшифровка подписи)

_____/ _____ /
(подпись) (расшифровка подписи)

[1] В случае уничтожения ПДн, обработка которых осуществлялась по поручению, указывается наименование лица, поручившего такую обработку

[2] Если невозможно перечислить ФИО всех субъектов, можно указать категорию субъектов (работники Оператора, родственники работников, контрагенты Оператора)

[3] Виды категорий ПДн: иные, специальные, биометрические