НОРНИКЕЛЬ

КОЛЬСКАЯ ГМК

Приложение 1

УТВЕРЖДЕНО
приказом Генерального директора
АО «Кольская ГМК»
От 25.05.2022 № КГМК/329-п

Положение

об организации обработки и обеспечении безопасности персональных данных в АО «Кольская горно-металлургическая компания»
П 156-23-2022

Обозначение документа: П 156-23-2022
Дата введения: 2022-05-25
Введено взамен: З 3-56-00-23-2020

Содержание

1. Область применения

1.1. Настоящее Положение об обработке и обеспечении безопасности персональных данных в АО «Кольская горно-металлургическая компания» (далее – Положение) устанавливает единые правила для процессов обработки персональных данных (далее – ПДн) и обеспечения безопасности персональных данных в АО «Кольская ГМК» (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 Общества с 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».

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.

1.5. Основные правила документирования деятельности, документооборота и обеспечения сохранности документов в Обществе установлены в Инструкции по делопроизводству в АО «Кольская ГМК», Регламенте согласование и утверждение приказов, распоряжений, нормативно-методических и организационно-правовых документов в АО «Кольская ГМК» и в Положении о порядке формирования документального фонда и организации архивного дела в АО «Кольская ГМК».

2. Нормативные ссылки*

При разработке Положения были использованы следующие нормативные

документы:

от 30.12.2001 № 197-ФЗ	Трудовой кодекс Российской Федерации (ТК РФ)
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» (149-ФЗ)
от 27.07.2006 № 152-ФЗ	Федеральный закон «О персональных данных» (152-ФЗ)
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»
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 167-003-2020	Регламент повышения осведомленности работников ПАО «ГМК «Норильский никель» в области информационной безопасности
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»
ПБП ГК НН 167-SFT.1.1.1-	Порядок управления доступом к информационным

2022	активам ПАО «ГМК «Норильский никель»
П 3-56-00-01-2018	Политика АО «Кольская горно-металлургическая компания» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных
П 179-19-2021	Положение о Комиссии по обеспечению безопасности персональных данных в АО «Кольская ГМК»
П 246-06-2021	Положение о порядке формирования документального фонда и организации архивного дела в АО «Кольская ГМК»
И 246-08-2020	Инструкция по делопроизводству в АО «Кольская ГМК»
Р 246-03-2020	Регламент согласование и утверждение приказов, распоряжений, нормативно-методических и организационно-правовых документов в АО «Кольская ГМК»

* в действующей редакции. При внесении изменений, пересмотре или замене указанных документов следует руководствоваться их актуализированными версиями, размещенными в ИС «Кодекс» и ИС ЭАНД «Алее Архив»

3. Термины, определения и сокращения

3.1. В настоящем Положении применены термины с соответствующими определениями:

3.1.1. **Аудит информационной безопасности:** систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации.

3.1.2. **Автоматизированная обработка персональных данных:** обработка персональных данных с помощью средств вычислительной техники.

3.1.3. **База данных:** представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

3.1.4. **Биометрические персональные данные:** сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

3.1.5. **Блокирование персональных данных:** временное прекращение обработки персональных данных (за исключением случаев, если обработка

необходима для уточнения персональных данных).

3.1.6. **Доступ к персональным данным:** возможность получения персональных данных и их использования.

3.1.7. **Доступность информации:** состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

3.1.8. **Запись персональных данных:** действия, направленные на фиксацию персональных данных на материальном носителе персональных данных или в информационной системе с целью их дальнейшего использования.

3.1.9. **Извлечение персональных данных:** действия, направленные на получение структурированных персональных данных из неструктурированных или слабоструктурированных машиночитаемых документов.

3.1.10. **Изменение персональных данных:** действия, направленные на модификацию значений персональных данных.

3.1.11. **Информационная безопасность:** защищенность информационных активов от случайных или преднамеренных угроз информационной безопасности, которые могут нанести ущерб Обществу и/или субъектам ее/их информационных отношений.

3.1.12. **Информационная система:** совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

3.1.13. **Информационная система персональных данных:** совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3.1.14. **Информационный актив:** информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации; находящаяся в распоряжении организации и представленная на любом материальном носителе персональных данных в пригодной для ее обработки, хранения или передачи форме.

3.1.15. **Информационные технологии:** процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Включают в себя: ИТ-инфраструктуру, информационные системы, цифровые системы и решения, средства метрологического обеспечения, средства промышленной автоматизации, средства телекоммуникации и связи, слаботочные системы.

3.1.16. **Информация:** сведения (сообщения, данные) независимо от формы их представления.

3.1.17. **Использование персональных данных:** действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

3.1.18. **ИТ-инфраструктура:** совокупность систем сбора, обработки, хранения и передачи данных. Включает в себя:

- инженерные системы обеспечения жизнедеятельности центров обработки данных, серверных и кроссовых помещений (системы кондиционирования, охлаждения, электропитания и т.д.);
- средства централизованного хранения и обработки данных (серверное

оборудование, системы резервного копирования, дисковые и ленточные массивы);

- системное и системообразующее программное обеспечение, системы виртуализации;
- системные каталоги (включая Active Directory);
- системы управления базами данных;
- средства вычислительной техники (рабочие станции, мониторы и периферийное оборудование, включая типовой комплект ПО рабочих мест пользователей;
- программно-аппаратный комплекс «киоски самообслуживания»;
- сети хранения данных;
- структурированные кабельные сети и системы управления коммутацией;
- локальные вычислительные сети (активное и пассивное оборудование);
- системы передачи данных и управления технологическим процессом;
- копировально-множительную аппаратуру (коллективного, группового и персонального пользования);
- средства связи (учрежденческие автоматические телефонные станции и их компоненты, стационарные телефоны и факсимильные аппараты, мобильные средства связи и др.) и видеосвязи;
- средства телекоммуникаций (каналы связи, телекоммуникационное оборудование);
- средства корпоративных коммуникаций (электронная почта и т.п.);
- системы управления и мониторинга компонентов инфраструктуры, ИТ-систем и ИТ-персонала;
- техническую и организационную документацию, связанную с эксплуатацией, поддержкой и сопровождением ИТ-систем и инженерных систем.

3.1.19. **ИТ-система:** совокупность технических средств и информационных объектов, взаимодействующих между собой для достижения общей цели, обладающая системным свойством (свойствами).

3.1.20. **Инцидент информационной безопасности:** событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности.

3.1.21. **Контролируемая зона:** пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств.

3.1.22. **Материальный носитель персональных данных:** материальный объект, используемый для закрепления и хранения на нем речевых, звуковых или изобразительных персональных данных, в том числе в преобразованном виде.

3.1.23. **Накопление персональных данных:** действия, направленные на формирование исходного, несистематизированного массива персональных данных.

3.1.24. **Неавтоматизированная обработка персональных данных (обработка персональных данных без использования средств автоматизации):** обработка персональных данных, содержащихся в информационных системах персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении

каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационных системах персональных данных либо были извлечены из нее.

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

3.1.26. **Обновление персональных данных:** проверка по имеющимся источникам актуальности уже хранящихся персональных данных и замена устаревших или некорректных персональных данных новым значениями.

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

3.1.28. **Обработчик персональных данных:** лицо, осуществляющее обработку персональных данных по поручению оператора.

3.1.29. **Объект доступа:** информационный актив, информационная система, бизнес-приложение, инфраструктурное приложение или компонент ИТ-инфраструктуры, автоматизированная система управления технологическим процессом, доступ к которым регламентируется правилами разграничения доступа.

3.1.30. **Общедоступные источники персональных данных:** содержащиеся в информационных системах или зафиксированные на материальных носителях персональных данных, доступ неограниченного круга лиц к которым предоставлен с письменного согласия субъекта этих персональных данных.

3.1.31. **Оператор (персональных данных):** государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

3.1.32. **Оператор информационной системы персональных данных:** физическое или юридическое лицо, осуществляющее деятельность по эксплуатации информационной системы персональных данных, в т.ч. по обработке персональных данных, содержащихся в ее базах данных. Если иное не установлено федеральными законами, оператором информационной системы персональных данных является собственник технических средств, используемых для обработки персональных данных, содержащихся в базах данных, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы персональных данных.

3.1.33. **Персональные данные:** любая информация, относящаяся к

прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

3.1.34. **Передача персональных данных:** распространение, предоставление или доступ к персональным данным.

3.1.35. **Предоставление персональных данных:** действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

3.1.36. **Программно-техническая база информационной системы персональных данных:** программные и технические средства информационной системы персональных данных, включая системное (в т.ч. операционная система), прикладное (в т.ч. система управления базами данных) и специальное программное обеспечение.

3.1.37. **Процесс обработки персональных данных:** бизнес-процесс АО «Кольская ГМК», в рамках которого осуществляется обработка персональных данных.

3.1.38. **Раскрытие персональных данных:** обеспечение доступа к персональным данным независимо от цели получения указанных персональных данных.

3.1.39. **Распространение персональных данных:** действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

3.1.40. **Сбор персональных данных:** действия, направленные на получение персональных данных.

3.1.41. **Система защиты персональных данных:** совокупность организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационной системе персональных данных, направленных на обеспечение безопасности персональных данных при их обработке в информационной системе персональных данных.

3.1.42. **Средства защиты информации:** технические, программные, программно-технические средства, предназначенные и используемые для защиты информации.

3.1.43. **Систематизация персональных данных:** действия, направленные на объединение и расположение персональных данных в определенной последовательности.

3.1.44. **Специальные категории персональных данных:** персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, о судимости.

3.1.45. **Субъект доступа:** лицо или процесс, действия которого регламентируются правилами разграничения доступа.

3.1.46. **Субъект персональных данных:** физическое лицо, которое прямо или косвенно определено, или определяемо с помощью персональных данных.

3.1.47. **Третьи лица:** любые физические лица, не являющиеся работниками Общества, любые юридические лица, их объединения, должностные лица, органы государственной власти и местного самоуправления, иные лица, с которыми Общество вступает в какие-либо правоотношения.

3.1.48. **Трансграничная передача персональных данных:** передача

персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3.1.49. **Целостность информации:** полнота, точность, непротиворечивость информации и отсутствие несанкционированных изменений при её передаче, обработке и хранении.

3.1.50. **Угрозы безопасности персональных данных:** совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

3.1.51. **Удаление персональных данных:** прекращение хранения персональных данных в рамках информационного актива.

3.1.52. **Уничтожение персональных данных:** действия, в результате которых становится невозможным восстановить содержание персональных данных в информационных системах персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3.1.53. **Уточнение персональных данных:** действия, направленные на обновление или изменение персональных данных.

3.1.54. **Хранение персональных данных:** действия, направленные на неизменность персональных данных, зафиксированных на материальном носителе персональных данных.

3.2. В настоящем Положении применены следующие сокращения:

БД	База данных
ВСП	Внутреннее структурное подразделение
ДБ	Департамент безопасности
ДПиСП	Департамент персонала и социальных политики
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
ИСПДн	Информационная система ПДн
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
ЛНА	Локальные нормативные акты Общества
Общество	АО «Кольская горно-металлургическая компания»
Обязательство об обеспечении	Обязательство лица, получившего доступ к ПДн, обеспечивать конфиденциальность и безопасность

конфиденциальности и безопасности ПДн	ПДн, в том числе: не разглашать ПДн; не передавать без служебной необходимости третьим лицам и не раскрывать публично ПДН; информировать непосредственного руководителя об утрате носителей ПДн и иных инцидентах информационной безопасности, связанных с Пдн
ОКА	Отдел кадрового администрирования Центра кадрового сервиса и социальных программ ДПиСП
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	Управление общественных связей 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
Работник безопасности ПДн при их обработке в ИСПДн в Обществе	Работник ДБ в Обществе, ответственный за определение мероприятий по обеспечению безопасности ПДн
Работник обработки ПДн в Обществе	Работники структурных и внутренних структурных подразделений Общества, в которых обрабатываются ПДн, ответственные за предоставление сведений об обрабатываемых ПДн в ИСПДн, заполнение и актуализацию карточек процессов обработки ПДн
РФ	Российская Федерация
СЗИ	Средства защиты информации
СЗПДн	Система защиты ПДн
СП	Структурное подразделение
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 Российской Федерации (Роскомнадзор)
Федеральный закон 152-ФЗ	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
RPO	Целевая точка восстановления (Recovery Point Objective)
RTO	Целевое время восстановления (Recovery Time Objective)

4. Общие положения

4.1. Бизнес-процессом 1-го уровня является бизнес-процесс «Обеспечение безопасности бизнеса».

4.2. Бизнес-процессом 2-го уровня является бизнес-процесс «Управление информационной безопасностью».

4.3. Владельцем системы управления ПДн является Заместитель генерального директора – директор департамента безопасности.

4.4. Основные принципы и условия обработки ПДн в Обществе установлены Политикой АО «Кольская ГМК» в отношении обработки персональных данных и сведения о реализации требованиях к защите персональных данных».

4.5. Отнесение сведений, обрабатываемых в Обществе, к ПДн и разделение их на категории осуществляется на основании классификационных признаков (критериев). Указанные критерии разрабатываются и актуализируются ДБ. на основании информации, предоставляемой подразделениями Общества, с учетом установленных в Обществе процедур и требований законодательства РФ в области ПДн.

4.6. В Обществе ведется Перечень подлежащих обработке ПДн Общества с учетом целей обработки ПДн, соответствующим деятельности, при которой такая обработка осуществляется.

4.7. В Обществе утверждается перечень лиц, доступ которых к ПДн, обрабатываемым в 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 заместителем генерального директора – директором ДПиСП Общества.

5. Структура и окружение системы управления ПДн

5.1. 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.

6. Функции участников

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

– Ответственный за организацию обработки ПДн в Обществе (п. 6.3 настоящего Положения);

– Ответственный за обеспечение безопасности ПДн в Обществе (п. 6.5 настоящего Положения);

– Подразделения, обеспечивающие эксплуатацию ИСПДн и ИТ-инфраструктуры в (п. 6.7 настоящего Положения);

– Подразделения, обеспечивающие эксплуатацию системы защиты ПДн (далее – СЗПДн) в (п. 6.8 настоящего Положения);

– Работник безопасности ПДн при их обработке в ИСПДн в Обществе (п. 6.9 настоящего Положения);

– Работник обработки ПДн в Обществе (п. 6.11 настоящего Положения);

– Работники правового департамента в Обществе (п. 6.13 настоящего Положения);

– Работники ОКА в Обществе (п. 6.14 настоящего Положения);

– Пользователи ПДн в Обществе (п. 6.15 настоящего Положения);

– Комиссия по обеспечению безопасности ПДн в Обществе (п. 6.17 настоящего Положения);

– Подразделение, организующее опубликование информации об условиях обработки ПДн в Обществе (п. 6.20 настоящего Положения).

6.2. Приказом генерального директора Общества могут быть предусмотрены дополнительные участники процессов обработки и обеспечения безопасности ПДн в Обществе.

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

6.4. Функции Ответственного за организацию обработки ПДн в Обществе установлены Политикой АО «Кольская горно-металлургическая компания» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных.

6.5. Ответственный за обеспечение безопасности ПДн в Обществе назначается приказом Генерального директора Общества.

6.6. Функции Ответственного за обеспечение безопасности ПДн в Обществе установлены Политикой АО «Кольская горно-металлургическая компания» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных.

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

– предоставление сведений работнику безопасности ПДн при их обработке в ИСПДн в Обществе для классификации 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 ЛНА Общества и эксплуатационной документацией;

– управление доступом Пользователей ПДн в Обществе к ИСПДн;

– управление средствами межсетевого экранирования и управление информационными потоками между ИСПДн;

– реализация защищенного доступа к ИСПДн;

– участие в определении ключевых параметров[1] 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;

– реализация антивирусной защиты;

– организация резервирования ПДн и ИСПДн;

– управление установкой (инсталляцией) компонентов 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 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.

6.8. 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;

---

[1] В определении ключевых параметров ИСПДн участвуют подразделения, обеспечивающие эксплуатацию ИСПДн в Обществе.

– 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;

– управление конфигурацией СЗПДн;

– осуществление мониторинга СЗПДн;

– формирование предложений по модернизации СЗПДн.

6.9. Работники безопасности ПДн при их обработке в ИСПДн в Обществе назначаются в Обществе приказом Генерального директора Общества или распоряжением Заместителя директора по безопасности.

6.10. Работники 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[2];

– 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 Работников обработки ПДн в Обществе и Подразделений, обеспечивающих эксплуатацию ИСПДн в Обществе;

– согласование доступа Пользователей ПДн в Обществе к 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;

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

– проведение мероприятий по внутреннему контролю и (или) аудитов ИБ

---

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

в части ПДн;

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

6.11. Работники обработки ПДн в Обществе назначаются:

– Заместителем генерального директора – директором ДПиСП или распоряжением руководителя СП, ВСП, осуществляющего обработку ПДн, с предоставлением копии в адрес Ответственного за обеспечение безопасности ПДн в Обществе.

6.12. Работники 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 СП, ВСП, 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 Работнику 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 ЛНА 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).

6.13. Работники правового департамента 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 ЛНА Общества и договоров Общества с третьими лицами на предмет их соответствия требованиям законодательства РФ в области ПДн.

6.14. Работники ОКА 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 ЛНА Общества в области ПДн.

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

6.16. 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 ЛНА Общества в части ПДн;

– участие во взаимодействии с субъектами ПДн;

– контроль точности, полноты и правильности ПДн, вводимых в ИСПДн.

6.17. Состав Комиссии по обеспечению безопасности ПДн в Обществе утверждается приказом Генерального директора Общества.

6.18. Дополнительно в Комиссию по обеспечению безопасности ПДн в Обществе могут быть включены работники СП, ВСП Общества, в которых осуществляется обработка ПДн.

6.19. Функции Комиссии по обеспечению безопасности ПДн в Обществе установлены Политикой АО «Кольская горно-металлургическая компания» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных и Положением о Комиссии по обеспечению безопасности персональных данных АО «Кольская ГМК».

6.20. Подразделение, организующее опубликование информации об условиях обработки ПДн в Обществе, в срок не позднее 2 (двух) рабочих дней с даты получения от Работников ОКА 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.

7. Требования к порядку обработки ПДн

7.1. Обработка ПДн осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом 152-ФЗ и ЛНА Общества. Обработка ПДн допускается в случаях, установленных частью 1 статьи 6 Федерального закона 152-ФЗ.

7.1.1. 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.

7.1.2. Формы согласий субъекта ПДн на обработку ПДн (исходя из целей обработки ПДн в Обществе), подлежащие применению в Обществе, а также правила их использования утверждаются приказом Генерального директора Общества.

7.1.3. Ответственным за разработку и актуализацию форм согласий субъекта ПДн на обработку ПДн является ДПиСП.

7.2. 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.

7.3. 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.

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

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

7.4.2. В поручении на обработку ПДн должны быть определены:

– 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).

7.5. 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.

7.6. Содержание и объем обрабатываемых ПДн должны соответствовать

заявленным целям обработки ПДн.

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

7.6.2. Работник обработки ПДн в Обществе и Пользователи ПДн в Обществе должны инициировать заполнение и поддерживать в актуальном состоянии карточки процессов обработки ПДн.

7.6.3. Карточка процесса обработки ПДн (Приложение А к настоящему Положению) включает в себя:

- цели осуществления обработки ПДн;
- правовые основания обработки ПДн;
- перечень обрабатываемых ПДн;
- перечень лиц и ВСП, СП, 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.

7.7. Особенности неавтоматизированной обработки ПДн:

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

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

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

7.7.4. 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.

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

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

7.7.7. 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.

7.7.8. 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».

7.7.9. 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.

7.7.10. 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.

7.8. Обработку ПДн могут осуществлять только Пользователи ПДн в Обществе, которым такая обработка необходима в связи с исполнением своих должностных обязанностей (при выполнении условий, предусмотренных в пунктах 12.2, 12.6 настоящего Положения).

7.8.1. Процедура предоставления доступа к ИСПДн Пользователей ПДн в Обществе определена ЛНА в области управления доступом к информационным активам Общества.

7.9. 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».

7.10. 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.

8. Особенности передачи ПДн

8.1. 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.

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

8.3. 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.

8.4. 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 РФ 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.

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

8.6. Трансграничная передача ПДн на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн, осуществляется в соответствии с Федеральным законом 152-ФЗ.

8.6.1. Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться в случаях:

– наличия согласия в письменной форме субъекта ПДн на трансграничную передачу его ПДн;

– предусмотренных международными договорами РФ;

– предусмотренных законодательством РФ, если это необходимо в целях защиты основ конституционного строя РФ, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

– исполнения договора, стороной которого является субъект ПДн;

– защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн.

8.7. В целях информационного обеспечения в Обществе 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.

8.8. Особенности обработки ПДн, разрешенных субъектом ПДн для распространения

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

8.8.2. 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.

8.8.3. 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.

9. Особенности удаления, уничтожения и обезличивания ПДн

9.1. 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.

9.2. 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.

9.3. Уничтожение ПДн должно производиться способом, исключающим возможность восстановления этих ПДн.

9.4. 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.

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

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

9.7. 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).

9.8. Требования к методам удаления, уничтожения и обезличивания ПДн устанавливаются соответствующим ЛНА Общества.

9.8.1. 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.

9.8.2. 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).

9.8.3. К требованиям к свойствам метода обезличивания относятся:

– обратимость (возможность проведения деобезличивания);

– возможность обеспечения заданного уровня анонимности;

– увеличение стойкости при увеличении объема обезличиваемых ПДн.

10. Взаимодействие с субъектами ПДн

10.1. 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 Обществе 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.

10.2. 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).

10.3. 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».

10.4. Запросы субъектов ПДн в Обществе 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.

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

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

11. Взаимодействие с органами государственной власти

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

11.2. 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.

11.3. 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.

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

11.5. 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.

12. Повышение осведомленности Пользователей ПДн в Обществе

12.1. 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».

12.2. В Обществе к обработке ПДн допускаются только лица, подписавшие обязательство об обеспечении конфиденциальности и безопасности ПДн Приложения Б, В к настоящему Положению.

12.3. При трудоустройстве работниками ОКА в Обществе осуществляется ознакомление трудоустраиваемых работников с утвержденными ЛНА Общества, устанавливающими требования и регламентирующими вопросы обработки и обеспечения безопасности ПДн в Обществе.

12.4. 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.

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

– требования законодательства РФ в области ПДн;

– правила обработки ПДн в Обществе;

– общие вопросы обеспечения ИБ в Обществе;

– ответственность за нарушение правил обработки и обеспечения безопасности ПДн.

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

– ознакомления с требованиями настоящего Положения, Политики АО «Кольская горно-металлургическая компания» в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных, иных ЛНА 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.

13. Обеспечение безопасности ПДн

13.1. 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».

13.2. 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.

13.3. 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.

13.4. 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.

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

13.4.2. 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.

13.4.3. 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.

13.4.4. 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.

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

13.4.6. 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.

13.4.7. 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.

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

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

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

– убытки[3] – 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,

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

если бы его право не было нарушено (упущенная выгода);

– моральный вред[4] – 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.

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

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

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

15.1. В целях соблюдения обязательных требований в области обработки и обеспечения безопасности ПДн в Обществе Ответственным за обеспечение безопасности ПДн в Обществе и Работником 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 СП, ВСП Общества требованиям законодательства РФ и ЛНА Общества в области ПДн;

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

– актуальности Перечня ПДн;

– актуальности Перечня лиц, допущенных к обработке ПДн;

– актуальности перечня ИСПДн;

– актуальности перечня СП, ВСП, участвующих в обработке ПДн в Обществе;

– 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;

– состояния мер обеспечения безопасности ПДн;

– состояния мер по соблюдению прав субъектов ПДн.

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

15.3. Ответственный за организацию безопасности ПДн в Обществе:

- ежегодно утверждает программу проведения мероприятий по внутреннему контролю и (или) аудитов ИБ (далее - программа аудита ИБ) в части ПДн;

- формирует предложения в отношении программы аудита ИБ и осуществляет подготовку ее проекта.

---

[4] Статья 151 Гражданского кодекса Российской Федерации.

15.4. 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 в Обществе.

15.5. 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.

15.6. 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 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.

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

15.8. 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.

15.9. В случае получения информации о факте нарушения действующего законодательства РФ и ЛНА Общества в области ПДн Ответственный за организацию обработки безопасности ПДн в Обществе 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.

15.10. Работник 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.

16. Ответственность

16.1. Ответственность за ненадлежащую организацию и неосуществление контроля исполнения требований настоящего Положения, а также за несвоевременное внесение изменение и дополнений в настоящее Положение несет лицо, ответственное за организацию обработки ПДн и лицо, ответственное за обеспечение безопасности ПДн Общества.

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

Приложение А

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 в Обществе
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 в Обществе

№	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 Б
Шаблон обязательства об обеспечении конфиденциальности и безопасности ПДн с работником

№_____ «____»_____ 20__ г.
дата регистрации

ОБЯЗАТЕЛЬСТВО ОБ ОБЕСПЕЧЕНИИ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я , _____ _____,
(фамилия, имя, отчество) *(табельный номер)*
документ, удостоверяющий личность_____ серия _____ № _____,
(вид документа)
выдан _____,
(кем и когда)
проживающий (ая) _____,
(адрес места жительства)
занимая должность _____

в структурном подразделении _____ (далее – Работник), как лицо, состоящее в трудовых отношениях с АО «Кольская горно-металлургическая компания» (далее – Работодатель), осознаю, что в процессе работы получу доступ к информации ограниченного доступа Работодателя, в том числе к персональным данным.

Я подтверждаю, что ознакомлен с «Политикой АО «Кольская горно-металлургическая компания» в отношении обработки персональных данных и сведениях о реализуемых требованиях к защите персональных данных», «Положением об организации обработки и обеспечения безопасности персональных данных» Работодателя, в которых определены порядок обращения с персональными данными и иные положения, касающиеся режима безопасности персональных данных Работодателя, а также с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, особенностями обработки персональных данных, установленными локальными нормативными актами Работодателя, и с обрабатываемыми категориями персональных данных.

Я подтверждаю, что не имею никаких обязательств перед каким-либо третьим лицом (физическим или юридическим), которые входят в противоречие с настоящим Обязательством или которые ограничивают мою деятельность на стороне Работодателя, и обязуюсь в период трудовых отношений с Работодателем (его правопреемником) и после их окончания:

- не разглашать персональные данные, ставшие мне известными в процессе выполнения моих трудовых обязанностей;
- не передавать третьим лицам и не раскрывать публично персональные данные;
- выполнять требования локальных нормативных актов Работодателя по обработке персональных данных и обеспечению защиты информации;
- в случае попытки посторонних лиц получить от меня персональные данные немедленно сообщить об этом непосредственному руководителю;
- в случае моего увольнения все носители персональных данных Работодателя: рукописи, черновики, документы и т. д., которые находились в моем распоряжении в связи с исполнением трудовых обязанностей во время работы, передать по акту непосредственному руководителю;
- об утрате или недостаче носителей персональных данных Работодателя, удостоверений, пропусков, ключей: от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению или утечке персональных данных, немедленно сообщить непосредственному руководителю.

Я согласен, что Работодатель будет осуществлять контроль процессов обработки мной персональных данных в целях выполнения требований законодательства и локальных нормативных актов Работодателя.

Я предупрежден о том, что в случае невыполнения мной любого из вышеперечисленных пунктов настоящего Обязательства и нарушения этих положений в отношении меня могут быть применены установленные законом меры ответственности, включая обязанность по возмещению Работодателю всех причиненных убытков.

«____»_____ 20__ г. _____ _____
Подпись *Расшифровка ФИО*

Приложение В
Шаблон обязательства об обеспечении конфиденциальности и безопасности ПДн (по договору ГПХ)

№_____ «____»_____ 20__ г.
дата регистрации

ОБЯЗАТЕЛЬСТВО ОБ ОБЕСПЕЧЕНИИ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____,
(фамилия, имя, отчество)
документ, удостоверяющий личность_____ серия _____№ _____,
(вид документа)
выдан _____,
(кем и когда)
проживающий (ая) _____,
(адрес места жительства)

(далее – Исполнитель), как лицо, заключившее гражданско-правовой договор с АО «Кольская горно-металлургическая компания», осознаю, что в процессе исполнения своих договорных обязательств получу доступ к информации ограниченного доступа АО «Кольская горно-металлургическая компания», в том числе к персональным данным.

Я подтверждаю, что ознакомлен с «Политикой АО «Кольская горно-металлургическая компания» в отношении обработки персональных данных и сведениях о реализуемых требованиях к защите персональных данных», «Положением об организации обработки и обеспечения безопасности персональных данных АО «Кольская горно-металлургическая компания», в которых определены порядок обращения с персональными данными и иные положения, касающиеся режима безопасности персональных данных АО «Кольская горно-металлургическая компания», а также с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, особенностями обработки персональных данных, установленными локальными нормативными актами АО «Кольская горно-металлургическая компания», и с обрабатываемыми категориями персональных данных.

Я подтверждаю, что не имею никаких обязательств перед каким-либо третьим лицом (физическим или юридическим), которые входят в противоречие с настоящим Обязательством или которые ограничивают мою деятельность на стороне АО «Кольская горно-металлургическая компания», и обязуюсь в период договорных отношений с АО «Кольская горно-металлургическая компания» (его правопреемником) и после их окончания:

- не разглашать персональные данные, ставшие мне известными в процессе выполнения моих договорных обязательств;
- не передавать третьим лицам и не раскрывать публично персональные данные;
- выполнять требования локальных нормативных актов АО «Кольская горно-металлургическая компания» по обработке персональных данных и обеспечению защиты информации;
- в случае попытки посторонних лиц получить от меня персональные данные немедленно сообщить об этом непосредственному руководителю;
- после прекращения гражданско-правовых отношений все носители персональных данных АО «Кольская горно-металлургическая компания»: рукописи, черновики, документы и т. д., которые находились в моем распоряжении в связи с исполнением договорных обязательств, передать по акту непосредственному руководителю;
- об утрате или недостаче носителей персональных данных АО «Кольская горно-металлургическая компания», удостоверений, пропусков, ключей: от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению или утечке персональных данных, немедленно сообщать непосредственному руководителю.

Я согласен, что АО «Кольская горно-металлургическая компания» будет осуществлять контроль процессов обработки мной персональных данных в целях выполнения требований законодательства и локальных нормативных актов АО «Кольская горно-металлургическая компания».

Я предупрежден о том, что в случае невыполнения мной любого из вышеперечисленных пунктов настоящего Обязательства и нарушения этих положений, в отношении меня могут быть применены установленные законом меры ответственности, включая обязанность по возмещению АО «Кольская горно-металлургическая компания» всех причиненных убытков.

«____»_____ 20__ г. _____ _____
Подпись *Расшифровка ФИО*