Приложение 1

УТВЕРЖДЕНА
приказом Президента
ПАО «ГМК «Норильский никель»
от 29.11.2017 №ГМК/136-п

ПОЛИТИКА

ПАО «ГМК «Норильский никель» в области обработки персональных данных

Обозначение документа: УП ГМК-НН 167-007-2017
Введена взамен: УП ГМК-НН 165-004-2014
Дата введения:

Содержание

1. Область применения

1.1. Настоящая Политика ПАО «ГМК «Норильский никель» в области обработки персональных данных (далее – Политика) определяет основные принципы и условия обработки персональных данных (далее – ПДн) в ПАО «ГМК «Норильский никель» (далее – Компания), а также меры по обеспечению безопасности ПДн в Компании.

1.2. Настоящая Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон), иных федеральных законов, регулирующих вопросы обработки ПДн, а также принятых в исполнение подзаконных нормативных правовых актов РФ.

1.3. Политика направлена на обеспечение прав и свобод человека и гражданина при обработке Компанией ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, в соответствии с требованиями действующего законодательства РФ.

1.4. Политика обязательна для исполнения всеми работниками Компании, участвующими в процессе обработки ПДн.

1.5. Политика публикуется на корпоративном сайте Компании в информационно-телекоммуникационной сети «Интернет» по адресу: www.nornickel.ru.

2. Нормативные ссылки

2.1. При разработке Политики были использованы следующие нормативные документы:

от 12.12.93	Конституция РФ
от 30.11.1994 № 51-ФЗ от 26.01.1996 № 14-ФЗ от 26.11.2001 № 146-ФЗ от 18.12.2006 № 230-ФЗ	Гражданский кодекс РФ
от 30.12.2001 № 197-ФЗ	Трудовой кодекс РФ
от 31.07.1998 N 146-ФЗ	Налоговый кодекс РФ
от 19.12.2005№ 160-ФЗ	Федеральный закон «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
от 27.07. 2007 № 152-ФЗ	Федеральный закон «О персональных данных»
от 01.04.1996 № 27-ФЗ	Федеральный закон «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»
от 22.10.2004 № 125-ФЗ	Федеральный закон «Об архивном деле в РФ»

от 21.07.1997 №116-ФЗ	Федеральный закон «О промышленной безопасности опасных производственных объектов»
от 21.07.1993 № 5485-1	Закон РФ «О государственной тайне»
от 31.05.1996 № 61-ФЗ	Федеральный закон «Об обороне»
от 12.02.1998 № 28-ФЗ	Федеральный закон «О гражданской обороне»
от 01.11.2012 №1119	Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
от 06.02.2010 № 63	Постановление Правительства РФ «Об утверждении Инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне»
от 27.11.2006 № 719	Постановление Правительства РФ «Об утверждении Положения о воинском учете»
ГОСТ Р ИСО/МЭК 27001-2006	Национальный стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
СТО ГМК-НН 20-002-2008	Стандарт организации «Нормативно-методическая и организационно-правовая документация. Общие требования к структуре и содержанию»

3. Термины, определения и сокращения

3.1. В настоящей Политике применены термины с соответствующими определениями:

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

3.1.2. **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).

3.1.3. **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.

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

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

3.1.6. **Конфиденциальность персональных данных:** обязательное для оператора и иных лиц, получивших доступ к персональным данным, требование не передавать третьим лицам персональные данные без согласия субъекта персональных данных или иного законного основания.

3.1.7. **Ответственный за организацию обработки персональных данных в Компании:** назначенный приказом Президента Компании работник ПАО «ГМК «Норильский никель», отвечающий за соблюдение ПАО «ГМК «Норильский никель» и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

3.1.8. **Несанкционированный доступ:** доступ к информации, ИТ-системам и компонентам ИТ-инфраструктуры лиц, не имеющих на это право, в нарушение правил разграничения доступа, но с использованием штатных средств, предоставляемых средствами вычислительной техники или информационной системы.

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

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

3.1.11. **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.

3.1.12. **Персональные данные:** любая информация, относящаяся к прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

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

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

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

3.1.16. **Структурное подразделение:** подразделение Компании, являющееся исполнителем отдельных процессов, функций, работ, участвующее в хозяйственной деятельности Компании, но не имеющее хозяйственной самостоятельности в рамках Компании.

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

3.1.18. **Трансграничная передача персональных данных:** передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или юридическому лицу.

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

3.1.20. **Угроза безопасности информации:** совокупность условий и факторов, определяющих наличие потенциальной или реально существующей опасности, связанной с реализацией риска информационной безопасности.

3.1.21. **Уничтожение персональных данных:** действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3.2. В настоящей Политике применены следующие сокращения:

Закон	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
ИСПДн	Информационная система персональных данных
Компания	ПАО «ГМК «Норильский никель»
РМД	Регламентирующие документы (нормативно-методические/организационно-правовые документы)
ПДн	Персональные данные
Политика	Политика ПАО «ГМК «Норильский никель» в области обработки персональных данных
РФ	Российская Федерация

4. Основные принципы Политики

4.1. Компания, являясь в соответствии с положениями Закона оператором ПДн, в своей деятельности обеспечивает соблюдение установленных Законом принципов обработки ПДн, описанных в пп. 4.1.1 – 4.1.7 настоящей Политики.

4.1.1. Обработка ПДн осуществляется на законной и справедливой основе.

4.1.2. Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не производится обработка ПДн, несовместимая с целями сбора ПДн.

4.1.3. Не производится объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.4. Обработке подвергаются только ПДн, которые отвечают целям их обработки.

4.1.5. Содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не являются избыточными по отношению к заявленным целям их обработки.

4.1.6. При обработке ПДн обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Компания принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

4.1.7. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн. Обрабатываемые ПДн уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.2. Требования по организации обработки и обеспечению безопасности ПДн в Компании определяются:

– требованиями ратифицированной РФ Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн;

– требованиями законодательства РФ в области ПДн, нормативно-методическими документами Компании и организационно-правовыми документами Компании;

– требованиями Трудового кодекса РФ;

– с учетом оценки вреда, который может быть причинен субъектам ПДн в случае нарушения действующего законодательства РФ;

– с учетом российских и международных стандартов в области ИБ.

4.3. С целью выполнения требований законодательства РФ в области ПДн в Компании действуют следующие процессы, связанные с обработкой и обеспечением безопасности ПДн:

– организация обработки ПДн;
– взаимодействие с субъектами ПДн;
– взаимодействие с органами государственной власти;
– повышение осведомленности пользователей ПДн[1];
– обеспечение безопасности ПДн;

[1] К пользователям ПДн относятся все работники Компании, участвующие в процессах обработки ПДн и допущенные к обработке ПДн.

– контроль за соблюдением требований в сфере обработки и защиты ПДн.

5. Объекты и субъекты Политики

5.1. Объектами Политики являются:

– ПДн, обрабатываемые в Компании;

– ИСПДн, функционирующие в Компании;

– требования по обеспечению безопасности ПДн при их обработке в ИСПДн, и системы защиты ПДн, функционирующие в Компании;

– нормативно-методические и организационно-правовые документы Компании в области ПДн.

5.2. С целью организации, контроля обработки и обеспечения безопасности ПДн в Компании определены следующие участники, являющиеся субъектами Политики:

– Ответственный за организацию обработки ПДн в Компании;

– Ответственные за обеспечение безопасности ПДн в Главном офисе, филиалах и представительстве Компании;

– Комиссия по обеспечению безопасности ПДн в Компании.

5.3. Ответственный за организацию обработки ПДн получает указания непосредственно от Президента Компании. Ответственному за организацию обработки ПДн предоставлены сведения, указанные в ч. 3 ст. 22 Закона.

5.4. Ответственный за организацию обработки ПДн в Компании выполняет следующие функции:

– организация разработки РМД Компании по вопросам обработки и обеспечения безопасности ПДн;

– консолидация перечня процессов обработки ПДн и перечня ИСПДн Компании и РОКС НН;

– организация проведения мероприятий по внутреннему контролю и (или) аудита ИБ на соответствие обработки ПДн требованиям законодательства РФ, а также утвержденными РМД Компании в области ПДн;

– организация оценки вреда, который может быть причинен субъектам ПДн в случае нарушения требований Закона, соотношение указанного вреда и принимаемых Компанией мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом;

– организация режима обеспечения безопасности помещений, в которых размещены ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– организация взаимодействия от имени Компании с Уполномоченным органом по защите прав субъектов ПДн и иными уполномоченными органами в случаях, предусмотренных законодательством РФ о ПДн, с привлечением работников правовых служб в ГО/филиалах/представительстве Компании;

– организация формирования и направления в Уполномоченный орган по защите прав субъектов ПДн в сроки, установленные Законом, уведомления об обработке Компанией (о намерении Компании осуществлять обработку) ПДн или информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн;

– осуществление регулярного мониторинга фактов включения Компании в ежегодный сводный план проведения плановых проверок субъектов предпринимательства на предмет соблюдения обязательных требований в области обработки ПДн;

– разработку и формирование плана и программы повышения осведомленности по вопросам обработки и обеспечения безопасности ПДн.

5.5. С целью обеспечения безопасности ПДн Ответственный за организацию обработки ПДн в Компании обеспечивает:

– вовлеченность руководителей Компании – деятельность по организации обработки и обеспечению безопасности ПДн инициируется и контролируется на уровне руководителей Компании;

– соответствие мер обеспечения безопасности ПДн требованиям законодательства РФ и РМД Компании в области ПДн;

– использование для обеспечения безопасности ПДн совокупности организационных и технических мер;

– повышение уровня осведомленности лиц, допущенных к обработке ПДн по вопросам обеспечения безопасности ПДн;

– постоянное совершенствование процессов обеспечения безопасности ПДн.

5.6. Ответственные за обеспечение безопасности ПДн в структурных подразделениях Компании выполняют следующие функции:

– организация работ по обеспечению безопасности ПДн;

– организация создания и ввода в эксплуатацию системы защиты ПДн, формирование предложений по модернизации системы защиты ПДн;

– организация управления инцидентами ИБ в ИСПДн;

– организация проверок соответствия обработки и обеспечения безопасности ПДн требованиям законодательства РФ и РМД Компании в области ПДн;

– организация информирования работников Компании о требованиях законодательства РФ в области обеспечения безопасности ПДн, а также РМД Компании по вопросам обеспечения безопасности ПДн.

5.7. Комиссия по обеспечению безопасности ПДн выполняет следующие функции:

– организация и участие в мероприятиях по определению ключевых сведений об ИСПДн;

– установление необходимого уровня защищенности ПДн при их обработке в ИСПДн;

– организация и проведение правовой оценки возможности создания (модернизации) ИСПДн, в том числе с учетом требований законодательства РФ и РНД Компании;

– проведение оценки вреда, который может быть причинен субъектами ПДн в случае нарушения действующего законодательства РФ в области ПДн;

– организация удаления, уничтожения ПДн, включая уничтожение бумажных носителей ПДн.

6. Основные положения об обработке ПДн

6.1. Обработка ПДн в Компании включает в себя любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, в том числе сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение ПДн.

6.2. Компания может осуществлять обработку биометрических ПДн только при наличии согласия в письменной форме субъекта ПДн.

6.3. Компания осуществляет обработку ПДн в случаях, определенных Законом.

6.4. Компания осуществляет обработку специальных категорий ПДн в случаях, определенных Законом.

6.5. Компания может осуществлять обработку ПДн о судимости субъекта ПДн только в случаях и в порядке, которые определяются в соответствии с федеральными законами РФ.

6.6. Обработка ПДн прекращается при достижении одного из следующих условий:

– достижение целей обработки ПДн и максимальных сроков хранения документов, их содержащих;

– утрата необходимости в достижении целей обработки ПДн;

– выявление неправомерной обработки ПДн;

– отзыв субъектом ПДн согласия на обработку ПДн, за исключением случаев, предусмотренных законодательством РФ в области ПДн.

6.7. Компания может осуществлять трансграничную передачу ПДн. До начала осуществления трансграничной передачи ПДн Компания обязана убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн. 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;

– 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;

– предусмотренных федеральными законами, 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.

6.8. Компания может создавать и использовать общедоступные источники ПДн, в которые включаются ПДн субъектов ПДн с их письменного согласия. Компания гарантирует исключение из общедоступных источников ПДн сведений о субъекте ПДн в любое время по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

6.9. Компания осуществляет обработку ПДн с использованием средств автоматизации и без использования средств автоматизации.

7. Сведения о соблюдении Компанией законодательно установленных прав субъектов ПДн

7.1. Компания при обработке ПДн гарантирует соблюдение всех законных прав субъектов ПДн.

7.2. Для получения доступа субъекта ПДн к его ПДн в соответствии с положениями ст. 14 Закона субъект ПДн, а также его законный представитель, вправе направить соответствующий положениям ст. 14 Закона официальный запрос на доступ к своим ПДн.

7.3. Запросы в части предоставления информации об обработке ПДн, а также запросы на уточнение, изменение или прекращение обработки ПДн и отзывы согласия на обработку ПДн направляются официальным письмом по адресу Компании, указанному в Едином государственном реестре юридических лиц, или по адресу: Российская Федерация, 123100, г. Москва, 1-й Красногвардейский пр., д. 15. Копии запросов и отзывов согласия для ускорения их рассмотрения по желанию субъекта ПДн могут быть направлены по адресу personal-data@nornik.ru.

7.4. Компания не осуществляет обработку ПДн без предварительного согласия субъекта ПДн в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации.

7.5. Компания не осуществляет принятие решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки ПДн.

7.6. Для реализации и защиты своих прав и законных интересов субъект ПДн имеет право обратиться к Компании. Компания рассматривает любые обращения и жалобы со стороны субъектов ПДн, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, применения мер ответственности к виновным лицам и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

7.7. Субъект ПДн вправе обжаловать действия или бездействие Компании путем обращения в уполномоченный орган по защите прав субъектов ПДн.

7.8. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

8. Сведения о принимаемых мерах по обеспечению выполнения Компанией обязанностей оператора при обработке ПДн

8.1. Компания принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, возложенных на нее в соответствии с действующим законодательством РФ в области ПДн, в том числе:

8.1.1. В Компании издаются и регулярно актуализируются документы, определяющие политику Компании в отношении обработки ПДн, нормативно-методические документы, устанавливающие правила обработки ПДн, а также нормативно-методические документы, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ в области ПДн, устранение последствий таких нарушений.

8.1.2. В Компании применяются организационные и технические меры по обеспечению безопасности ПДн в соответствии с ч. 2 ст. 19 Закона, в том числе:

- определяются угрозы безопасности ПДн при их обработке в информационных системах ПДн;
- применяются организационные и технические меры по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПДн;
- применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации при наличии обоснованной необходимости;
- производится оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;
- производится учет машинных носителей ПДн;
- производится обнаружение фактов несанкционированного доступа к ПДн и принимаются соответствующие меры;
- производится восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- производится установление правил доступа к ПДн, обрабатываемым в информационной системе ПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в информационной системе ПДн;
- производится контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн.

8.1.3. Осуществляется контроль соответствия обработки ПДн требованиям законодательства РФ в области ПДн и требованиям по защите ПДн.

8.1.4. Производится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона, соотношение указанного вреда и принимаемых Компанией мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом.

8.1.5. Производится ознакомление работников Компании, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ о ПДн, в том числе требованиями по защите ПДн,

документами, определяющими политику в отношении обработки ПДн, нормативно-методическими документами Компании по вопросам обработки ПДн и обеспечению безопасности ПДн и (или) обучение указанных работников.

8.1.6. При сборе ПДн Компания обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан РФ с использованием баз данных, находящихся на территории РФ.

8.1.7. Компания обязуется представить РНД Компании по вопросам обработки и обеспечения безопасности ПДн и (или) иным образом подтвердить принятие вышеуказанных мер по запросу уполномоченного органа по защите прав субъектов ПДн.

8.1.8. Компания выполняет свои обязанности, возникающие при обращении к нему субъекта ПДн или его представителя, а также уполномоченного органа по защите прав субъектов ПДн в соответствии с положениями Закона.

8.1.9. Компания выполняет свои обязанности по устранению нарушений законодательства РФ, допущенных при обработке ПДн, по уточнению, блокированию и уничтожению ПДн в соответствии с положениями Закона.

9. Ответственность

9.1. Ответственность за ненадлежащую организацию и неосуществление контроля исполнения требований настоящей Политики несет лицо, ответственное за организацию обработки ПДн.

9.2. Ответственность за несвоевременное внесение изменений и дополнений в настоящую Политику несет лицо, ответственное за организацию обработки ПДн.