Публичное акционерное общество
«ВЕРХ-ИСЕТСКИЙ ЗАВОД»

УТВЕРЖДАЮ

Генеральный директор

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Подлинник электронного документа хранится в системе электронного документооборота НЛМК@DOC

Идентификатор подписи **d41d6267-4002-4917-80c4-4be614ef2082**
Подписант **Доронин Е.С.**
Должность **Генеральный директор**
Дата подписания **17.08.2026 09:36 МСК**

Е.С. Доронин

17.08.2026

ПОЛОЖЕНИЕ

об обработке персональных данных

П 05757713-ES-34-0035-2026

(Взамен П LG-162-0006-2023 «Положение об обработке персональных данных»)

Введен в действие приказом от 27.08.2026 № 53-125-П-ОД
Дата введения: 01.09.2026

Содержание

1. ОБЛАСТЬ ПРИМЕНЕНИЯ 3
2. НОРМАТИВНЫЕ ССЫЛКИ 3
3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 3
4. СОКРАЩЕНИЯ 4
5. РОЛИ 4
6. ОТВЕТСТВЕННЫЕ ЗА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ 5
7. ПРАВОВЫЕ ОСНОВАНИЯ, ЦЕЛИ ОБРАБОТКИ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ/ОЦЕНКА ПРИМЕНИМОСТИ ТРЕБОВАНИЙ GDPR 5
8. СОГЛАСИЕ НА ОБРАБОТКУ 9
9. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 14
10. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПДн ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА 24
11. ОБУЧЕНИЕ ПЕРСОНАЛА ПРАВИЛАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 25
12. ТРЕБОВАНИЯ К ХРАНЕНИЮ ДОКУМЕНТОВ И ЗАПИСЕЙ 25
13. ОТВЕТСТВЕННОСТЬ 25
ПРИЛОЖЕНИЕ А (справочное) Термины и определения 26
ПРИЛОЖЕНИЕ Б (обязательное) Порядок назначения в компании ответственных лиц, их задачи, функции и права 28
ПРИЛОЖЕНИЕ В (обязательное) Матрица разграничения ответственности по процессам обработки и защиты ПДн 32
ПРИЛОЖЕНИЕ Г (обязательное) Форма согласия на обработку персональных данных для работников компании 34
ПРИЛОЖЕНИЕ Д (обязательное) Акт разъяснения субъекту персональных данных юридических последствий отзыва согласия на обработку персональных данных 36
ПРИЛОЖЕНИЕ Е (обязательное) Порядок взаимодействия с субъектами персональных данных 37
ПРИЛОЖЕНИЕ Ж (обязательное) Форма Обязательства о неразглашении персональных данных субъектов 40
ПРИЛОЖЕНИЕ И (обязательное) Форма поручения обработки персональных данных 41
ПРИЛОЖЕНИЕ К (обязательное) Форма акта об уничтожении персональных данных 46
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ К ПОЛОЖЕНИЮ 47
ЛИСТ РЕДАКЦИЙ ПОЛОЖЕНИЯ 47

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее Положение об обработке персональных данных (далее – положение) устанавливает порядок обработки персональных данных (ПДн) работников, бывших работников и иных субъектов, ПДн которые обрабатываются в компании, в процессе осуществления основной деятельности и подлежат защите в соответствии с Федеральным законом Российской Федерации №152-ФЗ «О персональных данных» (2.1.1), Трудовым кодексом Российской Федерации (2.1.2), нормативными актами Российской Федерации в области обработки и защиты ПДн, General Data Protection Regulation (EU) 2016/679 – Общим регламентом по защите данных (Регламент Европейского Союза 2016/679) (2.1.4) и применимыми требованиями законодательства иных стран.

1.2. Настоящее положение направлено на обеспечение соблюдения требований законодательства, применимого к обработке ПДн компанией, в рамках функционирования системы комплаенс компании.

2. НОРМАТИВНЫЕ ССЫЛКИ[1]

2.1. В настоящем положении использованы ссылки на следующие нормативные документы:

2.1.1. Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

2.1.2. Федеральный закон Российской Федерации от 30.12.2001 №197-ФЗ «Трудовой кодекс Российской Федерации».

2.1.3. Конституция Российской Федерации (принята на всенародном голосовании 12.12.1993).

2.1.4. General Data Protection Regulation (EU) 2016/679 – Общий регламент по защите данных (Регламент Европейского Союза 2016/679 от 27.04.2016).

2.1.5. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 №178 «Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона «О персональных данных».

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

3.1. В настоящем положении применены термины с соответствующими определениями (см. **приложение А**) в соответствии с Единым корпоративным глоссарием: **компания; функциональное направление**.

3.2. Дополнительно в настоящем положении применены термины с соответствующими определениями (см. **приложение А**): **автоматизированная обработка персональных данных; блокирование персональных данных; внутренняя типовая форма; информационная система персональных данных; инцидент; обезличивание персональных данных; обработка персональных данных; обработчик ('processor'); ограничение обработки; оператор ('controller'); переносимость персональных данных (right to data portability); персональные данные; предоставление персональных данных; прекращение обработки (обеспечение прекращения обработки) персональных данных; профилирование ('profiling'); процесс обработки персональных данных; распространение персональных данных; реестр персональных данных; совместный оператор ('joint controller'); согласие на обработку;**

[1] При пользовании настоящим документом необходимо проверить действие ссылочных нормативных документов в информационной системе общего пользования – на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или в официальной электронной базе организации-разработчика нормативного документа. Если ссылочный документ заменен (изменен), то при пользовании настоящим документом следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

трансграничная передача персональных данных; третье лицо; уничтожение персональных данных; Уполномоченный орган по защите прав субъектов персональных данных.

4. СОКРАЩЕНИЯ

4.1. В настоящем положении применены следующие сокращения:

4.1.1. **ЕС:** Европейский союз.

4.1.2. **ИБ**: Информационная безопасность.

4.1.3. **ИСПДн**: Информационная система персональных данных.

4.1.4. **ИС**: Информационная система.

4.1.5. **ПДн**: Персональные данные.

4.1.6. **СЗПДн**: система защиты персональных данных.

4.1.7. **GDPR**: General Data Protection Regulation (EU) Общий регламент по защите данных (2.1.4).

5. РОЛИ

5.1. Перечень ролей, используемых в настоящем положении, с определениями приведен в таблице 1.

Таблица 1 – Перечень ролей

Роль	Определение
Служба ИБ	Подразделение, на которое возложены функции по обеспечению ИБ в компании; подразделение, осуществляющее общее руководство обработкой и защитой ПДн в компании
Юридическая служба	Подразделение, осуществляющее правовое сопровождение деятельности компании
HR бизнес-партнер (HR БП)	Работник кадровой службы, отвечающий за организацию и координацию оказания кадровых услуг функциональному направлению (HR БП корпоративного уровня) или компании (HR БП локальный)
Субъект ПДн	Работник компании, бывший работник компании, контрагент, руководитель, участник (акционер) или работник юридического лица, являющегося контрагентом компании, иное лицо, чьи ПДн обрабатываются в компании
Ответственный за организацию обработки ПДн	Работник, осуществляющий организацию и контроль за реализацией мер по обеспечению обработки ПДн в компании
Ответственный за обеспечение безопасности ПДн	Работник, осуществляющий контроль над обеспечением безопасности ПДн в компании. Ответственный за обеспечение безопасности ПДн назначается из числа работников Службы ИБ
Комиссия по организации обработки и защиты ПДн	Постоянно действующий коллегиальный орган, созданный в целях контроля и координации действий структурных подразделений и должностных лиц компании по обеспечению требований законодательства в области обработки и защиты ПДн. Состав Комиссии определяется приказом руководителя компании. В состав комиссии входят представители Службы ИБ и Юридической службы

Роль	Определение
ООО «Центр корпоративных решений»[2]	Компания, оказывающая соответствующие, затрагиваемые в документе виды услуг в соответствии с договором на оказание услуг, заключенным между ООО «ЦКР» и настоящей компанией. Объем соответствующих услуг определяется договором на оказание услуг

6. ОТВЕТСТВЕННЫЕ ЗА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. С целью организации и контроля обработки ПДн в компании назначаются:

- Ответственный за организацию обработки ПДн;
- Ответственный за обеспечение безопасности ПДн (назначается при наличии требований по обеспечению соответствующего уровня защищенности ПДн при их обработке в ИСПДн).

6.2. Порядок назначения в компании ответственных лиц, их задачи, функции и права изложены в **приложении Б**.

6.3. Порядок взаимодействия по процессам обработки и защиты ПДн в компании приведен в Матрице разграничения ответственности в **приложении В**.

7. ПРАВОВЫЕ ОСНОВАНИЯ, ЦЕЛИ ОБРАБОТКИ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ/ОЦЕНКА ПРИМЕНИМОСТИ ТРЕБОВАНИЙ GDPR

7.1. Правовые основания обработки персональных данных

7.1.1. Компания имеет право обрабатывать ПДн в случае, если применимо одно из следующих оснований обработки:

- субъект ПДн дал свое согласие на обработку своих ПДн для одной или нескольких конкретных целей;
- обработка ПДн необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на оператора (компанию) функций, полномочий и обязанностей;
- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- обработка необходима для выполнения требований законодательства ЕС или иной страны, под действие которого подпадает компания;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- обработка необходима для осуществления законных интересов компании или третьей стороны, за исключением случаев, когда такие интересы перекрываются интересами или основными правами и свободами субъекта ПДн;
- обработка ПДн необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве;

[2] Все ссылки на ООО «ЦКР» в настоящем документе и приложениях к нему являются ссылками на ООО «ЦКР как на лицо, оказывающее соответствующий, затрагиваемый в документе вид услуг в соответствии с договором на оказание услуг, заключенным между ООО «ЦКР» и Обществом. Объем соответствующих услуг определяется договором на оказание услуг.

- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;
- а также в иных случаях, предусмотренных действующим законодательством РФ, ЕС или иной страны, под действие которого подпадает компания.

7.2. Цели обработки персональных данных

7.2.1. Цели обработки ПДн установлены «Политикой в области обработки и защиты персональных данных»[3].

7.2.2. Если обработка ПДн подпадает под действие GDPR, то обработка ПДн в целях, отличных от изначальных целей их сбора, допускается только в случае совместимости новых и изначальных целей. Если цели совместимы, обработка ПДн для новой цели может выполняться на законном основании, действующем для изначальной цели.

7.2.3. При оценке совместимости целей обработки ПДн рассматривают следующие факторы:

- наличие связей между изначальными и новыми целями обработки ПДн;
- контекст, в котором были собраны ПДн, в частности, разумные ожидания субъекта ПДн от их дальнейшего использования компанией, которые основываются на взаимоотношениях между субъектом и компанией;
- состав ПДн, в частности, обрабатываются ли специальные категории ПДн или ПДн о судимостях и правонарушениях;
- последствия предлагаемой обработки для субъектов ПДн;
- наличие соизмеримых мер защиты ПДн в текущих и планируемых процессах обработки.

7.2.4. Решение о совместимости целей обработки принимают совместно Ответственный за организацию обработки ПДн и Юридическая служба.

7.3. Состав персональных данных

7.3.1. Компания не получает и не обрабатывает ПДн субъекта о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации (2.1.3), компания вправе получать и обрабатывать данные о частной жизни сотрудника только с его письменного согласия.

7.3.2. Компания не имеет права получать и обрабатывать ПДн субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных применимым законодательством.

7.3.3. Состав получаемых компанией ПДн является ограниченным, адекватным и релевантным по отношению к целям их обработки (принцип минимизации состава обрабатываемых данных – «data minimisation»).

7.3.4. Состав обрабатываемых в компании ПДн определяется Перечнем обрабатываемых ПДн и Реестром ПДн, подлежащих защите в соответствии с GDPR, которые утверждаются Ответственным за организацию обработки ПДн. Актуальное состояние документов поддерживается Службой ИБ и подлежит согласованию с Юридической службой. Перечень и Реестр ПДн подлежат плановому ежегодному пересмотру. Внеплановый пересмотр проводится при изменении информации о процессах обработки ПДн, состава ПДн, целей обработки и т.д.

[3] Политика LG-162-0001-2019 «Политика в области обработки и защиты персональных данных компаний Группы НЛМК» (приказ от 04.02.2019 №48).

7.3.5. В Перечне обрабатываемых ПДн должны быть отражены следующие сведения:

- категории субъектов ПДн;
- цели обработки ПДн;
- состав ПДн;
- наименования ИСПДн, в которой обрабатываются ПДн, в случае автоматизированной обработки;
- сроки хранения ПДн и нормативные документы, определяющие сроки хранения ПДн (при наличии);
- условия прекращения обработки ПДн.

7.3.6. В Реестре ПДн, подлежащих защите в соответствии с GDPR, должны быть отражены следующие сведения:

- наименование и контактная информация оператора ПДн и, если применимо, совместного оператора, представителя оператора и ответственного за защиту данных (DPO);
- цели обработки ПДн;
- законные основания обработки;
- категории субъектов ПДн;
- состав ПДн;
- операции по обработке ПДн;
- объем обрабатываемых ПДн;
- ИСПДн, в которых обрабатываются ПДн;
- категории и перечень третьих сторон, которым передаются ПДн, в т.ч. расположенные в других странах и международные организации;
- где применимо, наличие трансграничной передачи ПДн с указанием страны или международной организации, а также, если применимо, используемых законных оснований для передачи (safeguards);
- где возможно, сроки хранения ПДн;
- где возможно, общее описание технических и организационных мер защиты данных (security of processing)».

7.4. Оценка вреда, который может быть причинен субъектам ПДн

7.4.1. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона «О персональных данных» (2.1.1) (далее – оценка вреда) осуществляется в случае проектирования нового или изменении текущего бизнес-процесса, в рамках которого появляются новые категории ПДн, и в иных установленных законом случаях.

7.4.2. Оценку вреда проводит Комиссия по организации обработки и защите ПДн в соответствии с требованиями Приказа (2.1.5).

7.4.3. Результаты оценки вреда оформляют актом оценки вреда, который должен содержать:

- наименование и адрес оператора;
- дату издания акта оценки вреда;
- дату проведения оценки вреда;

- фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;
- степень вреда, которая может быть причинена субъекту ПДн.

7.5. Оценка на соответствие требованиям законодательства в области защищенности и правомерности обработки ПДн

7.5.1. В случае проектирования нового или изменения текущего бизнес-процесса, при котором появляются:

- новые цели обработки ПДн;
- новые категории субъектов ПДн;
- расширяется и/или изменяется перечень обрабатываемых ПДн;
- расширяется и/или изменяется перечень операций, осуществляемых с ПДн;
- меняется перечень третьих лиц, которым передаются ПДн;
- иные изменения с ПДн,

Юридическая служба совместно со Службой ИБ проводит оценку защищенности и правомерности обработки ПДн.

7.5.2. Внедрение новых или изменение текущих бизнес-процессов, при которых затрагиваются вышеуказанные действия с ПДн, производится при условии наличия оценки защищенности и правомерности обработки ПДн.

7.5.3. Оценка защищенности и правомерности обработки ПДн проводится в свободной форме и должна включать в себя как минимум следующее:

- анализ на соответствие принципам обработки (оценка необходимости и пропорциональности обработки ПДн относительно целей их обработки, точность данных, ограничение срока хранения и др.);
- оценку законности обработки ПДн с учетом требований применимого законодательства РФ и иных стран, под действие которого подпадает компания;
- оценку обеспечения безопасности данных;
- оценку внутреннего (организационные/технологические изменения, ресурсы компании, политика компании по основным направлениям деятельности и др.) и внешнего (появление новых законодательных требований, новых стандартов поведения в области ПДн, новых технологий и т.д.) контекстов;
- выявление потенциальных уязвимостей процесса, которые существуют или могут существовать;
- меры, предусмотренные для устранения выявленных несоответствий (если применимо), включая меры и механизмы обеспечения защиты ПДн или подтверждение соблюдения требований применимого законодательства в области ПДн.

7.5.4. С целью проведения процедуры по оценке защищенности и правомерности обработки ПДн структурное подразделение, осуществляющее проектирование нового или изменение текущего процесса, в котором осуществляется обработка ПДн, на этапе подготовительных работ до внедрения процесса в работу направляет в Юридическую службу обращение с обязательным указанием следующих данных:

- цель обработки ПДн;
- категории субъектов ПДн;
- перечень обрабатываемых ПДн;

- операции, осуществляемые с ПДн (сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных);
- правовое основание обработки ПДн (согласие, договор или иное);
- описание бизнес-процесса, в рамках которого осуществляется обработка ПДн;
- при осуществлении передачи ПДн третьим лицам необходимо указать полное наименование третьего лица и цель передачи данных;
- срок хранения данных;
- форма хранения данных (электронная с указанием ИСПДн или бумажная);
- наличие/отсутствие передачи данных за пределы РФ.

7.5.5. Юридическая служба вправе запрашивать дополнительную информацию, не указанную в обращении, но необходимую для проведения оценки.

7.5.6. Юридическая служба совместно со Службой ИБ в течение 15 рабочих дней с момента получения данных от структурного подразделения, проводит соответствующую оценку и в течение 3 рабочих дней с момента окончания проведения оценки направляет результаты оценки заявителю обращения.

8. СОГЛАСИЕ НА ОБРАБОТКУ

8.1. Общие положения

8.1.1. В случае, когда обработка ПДн возможна в соответствии с применимым законодательством или настоящим положением только при условии получения согласия на обработку, лицо, ответственное за взаимодействие с субъектом и/или инициирующее обработку ПДн, обязано обеспечить получение согласия на обработку от субъекта ПДн до начала обработки ПДн.

8.1.2. Согласие на обработку должно быть получено либо в письменной форме с подписью субъекта ПДн, либо в электронной форме, предоставляющей достаточный уровень уверенности в том, что согласие подписано субъектом ПДн. Согласие на обработку персональных данных должно быть оформлено отдельно от иных информации и (или) документов, которые подтверждает и (или) подписывает субъект персональных данных. Согласие запрещено включать в текст каких-либо документов – трудового договора, договора оказания услуг, заявления или иного документа, подписываемого субъектом ПДн, даже в виде отдельного пункта или приложения внутри этого документа.

8.2. Содержание согласия субъекта на обработку ПДн по требованиям законодательства РФ

8.2.1. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным.

8.2.2. Форма согласия на обработку ПДн включает следующую информацию:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);

- наименование и контактные данные компании, являющейся оператором ПДн;
- цели обработки персональных данных;
- перечень операций по обработке персональных данных;
- категории и перечень обрабатываемых данных;
- наличие у субъекта права на отзыв согласия и способ такого отзыва;
- срок, на который дается согласие.

8.2.3. Форма согласия на обработку ПДн для работников компании приведена в **приложении Г**.

8.2.4. Иные формы согласий на обработку ПДн разрабатывает Юридическая служба по обращениям структурных подразделений в течение 10 рабочих дней с даты получения обращения. Такое обращение должно содержать следующую информацию:

- цель обработки ПДн;
- категорию субъекта ПДн (работник, контрагент или иное);
- перечень обрабатываемых ПДн;
- операции, осуществляемые с ПДн (сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных);
- информацию о наличии автоматизированного принятия решения на основании собираемых ПДн (применимо для случаев, когда осуществляется обработка ПДн граждан, находящихся на территории ЕС);
- при осуществлении передачи ПДн третьим лицам необходимо указать полное наименование третьего лица и цель передачи данных;
- срок хранения ПДн.

8.3. Содержание согласия субъекта на обработку ПДн по требованиям GDPR

8.3.1. Согласие субъекта на обработку ПДн должно быть свободно данным – предоставление или отказ от предоставления субъектом согласия на обработку ПДн не должно оказывать влияние на реализацию субъектом своих прав и свобод.

8.3.2. Согласие на обработку ПДн должно содержать описание конкретных целей обработки ПДн, быть конкретным и недвусмысленным. При этом, должны соблюдаться следующие требования:

- степень детализации целей должна быть достаточной, чтобы препятствовать двоякому толкованию целей или их размытию и подтверждать соблюдение принципа «ограничение целей обработки»;
- в случае, если согласие запрашивается для нескольких целей единовременно, такое согласие должно включать отдельное подтверждающее действие на каждую из целей обработки, т.е. предоставлять субъекту возможность дать выборочное согласие;
- согласие должно содержать описание категорий ПДн, которые требуются для достижения каждой конкретной цели обработки.

8.3.3. Согласие на обработку ПДн должно предоставлять субъекту достаточный объем информации для принятия информированного решения. Компания должна предоставить субъекту достаточный объем информации об обработке ПДн, на которую запрашивается согласие, перед получением такого согласия. В частности, форма должна включать следующую информацию:

- наименование и контактные данные компании, являющейся оператором (‘controller’) ПДн;
- цели выполнения конкретных операций по обработке ПДн;
- состав или категории, собираемых ПДн;
- наличие у субъекта права отзыва согласия;
- информацию о наличии автоматизированного принятия решений на основании собираемых ПДн (если применимо);
- возможные риски, связанные с передачей ПДн третьим лицам, в случае, если в отношении них отсутствует решение Европейской комиссии об обеспечении адекватного уровня защиты данных.

8.3.4. Согласие на обработку ПДн должно быть доступным и понятным для субъекта ПДн, составлено на простом и понятном языке с учетом особенностей категории субъектов ПДн.

8.3.5. Согласие на обработку ПДн должно быть явным изъявлением воли субъекта ПДн. Субъект должен подтверждать согласие на обработку ПДн путем совершения конкретного действия, которое четко указывает на то, что субъект в указанном контексте согласен на запланированную обработку своих ПДн. В отдельных случаях обработки ПДн, компания должна запрашивать у субъекта ПДн явную форму согласия (‘explicit consent’). В частности, явная форма согласия требуется в следующих случаях, когда:

- оператор намерен обрабатывать специальные категории ПДн на основании согласия субъекта;
- оператор запрашивает согласие на обработку ПДн, включающую в себя трансграничную передачу ПДн в страны или международные организации, в отношении которых отсутствует решение Европейской Комиссии об обеспечении адекватной защиты данных или которые не предоставляют требуемых гарантий защиты данных, а также соблюдены иные требования законодательства о трансграничной передаче;
- оператор запрашивает согласие на выполнение операций автоматизированного принятия решений, включая профилирование, на основании собираемых ПДн.

8.4. Порядок отзыва согласия на обработку ПДн

8.4.1. Субъект ПДн или его представитель вправе отозвать согласие на обработку ПДн путем направления в адрес оператора письменного уведомления в форме:

- бумажного документа;
- электронного документа, который должен быть подписан электронной подписью субъекта ПДн в соответствии с законодательством РФ.

8.4.2. Структурное подразделение, получившее отзыв согласия субъекта на обработку ПДн, незамедлительно информирует по электронной почте о поступлении отзыва согласия Юридическую службу.

8.4.3. В случае, если субъект, направивший отзыв согласия на обработку ПДн, является работником компании, Юридическая служба информирует:

- руководителя структурного подразделения субъекта ПДн;
- HR БП курирующего подразделение;
- представителя Службы ИБ.

8.4.4. В рамках рассмотрения отзыва согласия субъекта на обработку ПДн представители Юридической службы и Службы ИБ в течение 3 (трех) рабочих дней с даты получения отзыва согласия:

- определяют перечень подлежащих прекращению обработки ПДн субъекта и/или наличие иных оснований для обработки ПДн в соответствии с законодательством РФ;
- с участием HR БП проводят собеседование (очно или дистанционно) с субъектом ПДн или его представителем для разъяснения юридических последствий отзыва согласия на обработку ПДн и/или информирования о наличии иных законных оснований для обработки его ПДн, в соответствии с которыми Оператор вправе продолжить обработку ПДн без его согласия, если таковые имеются.

8.4.5. По результатам собеседования Юридическая служба и Служба ИБ составляют акт по приведенной в **приложении Д** форме, в котором указывается подтверждение решения субъекта ПДн или его представителя об отзыве согласия на обработку ПДн или его отмена. Если субъект ПДн или его представитель отказывается участвовать или не является на назначенное собеседование, считается, что он осознает юридические последствия отзыва согласия на обработку ПДн и подтверждает его.

8.4.6. Данный акт и заявление субъекта об отзыве согласия на обработку ПДн HR БП передает в ООО «ЦКР» для хранения в личном деле работника / бывшего работника Оператора.

8.4.7. В случае подтверждения субъектом ПДн или его представителем решения об отзыве согласия на обработку ПДн Оператор прекращает обработку ПДн или должен обеспечить прекращение такой обработки (если обработка осуществляется обработчиком), в течение 10 (десяти) рабочих дней с даты получения отзыва согласия. Указанный срок может быть продлен не более чем на 5 (пять) рабочих дней по мотивированному уведомлению, которое Оператор должен направить в адрес субъекта ПДн.

8.4.8. Для обеспечения прекращения обработки ПДн данного субъекта представитель Юридической службы направляет соответствующее поручение в ООО «ЦКР» и структурные подразделения (при необходимости) с указанием срока прекращения обработки. В случае если ПДн субъекта обрабатываются третьим лицом по поручению, структурное подразделение, являющееся инициатором этого поручения, направляет обработчику информацию о необходимости прекращения обработки с указанием срока прекращения обработки, и получает от обработчика подтверждение уничтожения ПДн субъекта. Подтверждением уничтожения субъекта ПДн является Акт об уничтожении ПДн и выгрузка из журнала регистрации событий в информационной системе ПДн (в случае автоматизированной обработки ПДн). Копии полученных от обработчика Акта и выгрузки из журнала структурное подразделение направляет в Службу ИБ для хранения.

8.4.9. В случае, если субъект, направивший отзыв согласия на обработку ПДн, не является работником компании, Юридическая служба информирует представителя Службы ИБ.

8.4.10. В рамках рассмотрения отзыва согласия субъекта на обработку ПДн представители Юридической службы и Службы ИБ в течение 3 (трех) рабочих дней с даты получения отзыва согласия определяют перечень подлежащих прекращению обработки ПДн субъекта и/или наличие иных оснований для обработки ПДн в соответствии с законодательством РФ.

8.4.11. В случае отсутствия законных оснований для дальнейшей обработки ПДн Оператор прекращает обработку ПДн или должен обеспечить прекращение такой обработки (если обработка осуществляется обработчиком), в течение 10 (десяти) рабочих дней с даты

получения отзыва согласия. Указанный срок может быть продлен не более чем на 5 (пять) рабочих дней по мотивированному уведомлению, которое Оператор должен направить в адрес субъекта ПДн.

8.4.12. Для обеспечения прекращения обработки ПДн данного субъекта представитель Юридической службы направляет соответствующее поручение в структурные подразделения (при необходимости) с указанием срока прекращения обработки. В случае если ПДн субъекта обрабатываются третьим лицом по поручению, структурное подразделение, являющееся инициатором этого поручения, направляет обработчику информацию о необходимости прекращения обработки с указанием срока прекращения обработки, и получает от обработчика подтверждение уничтожения ПДн субъекта. Подтверждением уничтожения субъекта ПДн является Акт об уничтожении ПДн и выгрузка из журнала регистрации событий в информационной системе ПДн (в случае автоматизированной обработки ПДн). Копии полученных от обработчика Акта и выгрузки из журнала структурное подразделение направляет в Службу ИБ для хранения.

8.4.13. Прекращение обработки ПДн может быть обеспечено уничтожением или, если уничтожение по каким-то причинам невозможно, блокированием в порядке, установленном в п.9.8-9.9 настоящего положения. После выполнения мероприятий по прекращению обработки ПДн субъекта структурные подразделения информируют Юридическую службу и Службу ИБ о выбранном способе прекращения обработки ПДн субъекта (уничтожение или блокирование), а также о фактическом прекращении обработки ПДн субъекта с предоставлением подтверждающих документов. Подтверждением уничтожения субъекта ПДн является Акт об уничтожении ПДн и выгрузка из журнала регистрации событий в информационной системе ПДн (в случае автоматизированной обработки ПДн).

8.4.14. После получения документов, подтверждающих прекращение обработки, представитель Юридической службы готовит ответ субъекту ПДн на поступивший от него отзыв согласия.

8.4.15. Ответ подписывается лицом, на которого был направлен отзыв согласия субъекта ПДн или иным лицом, имеющим полномочия на подписание отзыва, и направляется субъекту ПДн не позднее 10 (десяти) рабочих дней с даты получения отзыва согласия или 15 (пятнадцати) рабочих дней, если срок был продлен по мотивированному уведомлению. Ответственным за отправку является:

- HR BP – в случае если субъект, направивший отзыв согласия на обработку ПДн, является работником компании. В этом случае HR BP также направляет копию ответа в ООО «ЦКР» для хранения в личном деле;
- Представитель структурного подразделения, получившее отзыв согласия субъекта на обработку ПДн, – в случае если субъект, направивший отзыв согласия на обработку Пдн, не является работником компании.

8.4.16. Копия ответа и актов об уничтожении ПДн хранятся в ООО «ЦКР» в личном деле работника/бывшего работника Оператора, для субъектов ПДн, не являющихся работником компании, – в Юридической службе.

9. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Общая информация по обработке ПДн

9.1.1. Компания осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

9.1.2. Компания прекращает обработку ПДн по требованию субъекта ПДн в пределах сроков, указанных в п.8.3, если иной срок не установлен требованиями действующего законодательства РФ.

9.1.3. Компания осуществляет обработку ПДн с использованием средств автоматизации и без использования таких средств в соответствии с требованиями действующего законодательства.

9.1.4. Компания планирует соответствующие организационные и технические меры защиты ПДн на стадии проектирования процессов обработки ПДн. Меры по обеспечению безопасности ПДн реализуются, в том числе, посредством применения в ИСПДн средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности ПДн и экономически целесообразно. Управление мерами обеспечения информационной безопасности ПДн проводится в соответствии с документом, определяющим политику информационной безопасности компании.

9.2. Сбор персональных данных

9.2.1. Компания получает ПДн непосредственно от субъекта ПДн, а также от третьего лица, в целях исполнения договорных обязательств, исполнения требований федерального законодательства, а также осуществления законных интересов компании.

9.2.2. По запросу субъекта ПДн компания сообщает ему о целях, способах, источниках получения ПДн и возможных последствиях отказа субъекта дать согласие на их получение и обработку, если в соответствии с Федеральным законом «О персональных данных» (2.1.1) получение Оператором согласия на обработку ПДн является обязательным. Взаимодействие с субъектами ПДн осуществляется в соответствии с **приложением Е**.

9.2.3. Субъект, являющийся работником компании, обязан предоставлять достоверные сведения о себе и в случае их изменения информировать о данном факте компанию в течение 10-и рабочих дней с даты такого изменения. Компания имеет право проверять достоверность сведений, предоставленных субъектом, путем сверки с документами.

9.2.4. ПДн субъектов могут быть получены не от самого субъекта, а от третьего лица только в том случае, если получение их у самого субъекта затруднительно. При этом ПДн не от самого субъекта могут быть получены компанией на основании федерального законодательства, а также в случае, если эти ПДн являются общедоступными.

9.2.5. Если ПДн получены не от субъекта ПДн, до начала обработки таких ПДн компания обязана предоставить субъекту ПДн следующую информацию:

- наименование и адрес оператора или его представителя;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные Федеральным законом «О персональных данных» (2.1.1) права субъекта ПДн.

Указанные сведения передаются субъекту в форме уведомления с использованием доступных каналов связи.

9.2.6. Если обрабатываемые ПДн подпадают под действие GDPR, компания уведомляет субъектов ПДн об обработке ПДн как при получении данных непосредственно от субъекта, так и при получении данных из прочих источников. Уведомления об обработке ПДн должны содержать:

- наименование и контактную информацию компании, а также представителя компании (где применимо);
- цели обработки, для достижения которых собираются ПДн, и законные основания обработки;
- перечень получателей или категории получателей ПДн;
- информацию о законных интересах компании, относящихся к обработке ПДн;
- четкое определение срока хранения ПДн или, если установление конкретного срока невозможно, критерии, используемые для определения такого срока;
- информацию о наличии у субъекта данных права доступа к ПДн, исправления или удаления ПДн, ограничения обработки ПДн; о праве субъекта выразить несогласие с обработкой ПДн, а также о праве на переносимость ПДн (в случае, если обработка ПДн выполняется на основании согласия субъекта или на основании заключенного договора с субъектом);
- информацию о праве отзыва согласия на обработку ПДн (в случае, если обработка ПДн выполняется на основании согласия субъекта);
- информацию о праве подачи жалобы в надзорный орган;
- информацию об источнике получения ПДн (при получении ПДн субъекта от третьего лица);
- информацию о наличии принятия решений, имеющих юридические или иные значимые последствия для субъекта ПДн, на основании только автоматизированной обработки его ПДн, а также об операциях профилирования.

9.2.7. Компания поддерживает актуальность уведомлений об обработке ПДн и обеспечивает оперативное информирование субъектов в случае их изменения за счет внедрения соответствующих процессов.

9.2.8. ПДн должны быть точными и, где необходимо, поддерживаться в актуальном состоянии. Компания предусматривает процедуры проверки корректности и обновления ПДн сотрудников и третьих лиц в ИС, справочниках, структурах учета и хранения документов, в том числе принимает обоснованные меры для обеспечения своевременного удаления или исправления ПДн, которые являются не точными по отношению к целям их обработки.

9.2.9. Если ПДн раскрываются третьим лицам, компания обязана уведомить об исправлении всех получателей ПДн.

9.3. Накопление персональных данных

9.3.1. Накопление ПДн происходит в результате основной деятельности компании следующими способами:

- внесение сведений в структуры хранения и учета документов («filing system»);
- получение оригиналов документов (анкета и пр.).

9.4. Хранение персональных данных

9.4.1. ПДн в компании хранят в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, после чего данные могут быть обезличены (при необходимости) или уничтожены в установленном порядке.

9.4.2. Хранение не конфиденциальных документов вместе с конфиденциальными документами, содержащими ПДн, разрешено только в случаях, когда они являются приложениями к конфиденциальным документам.

9.4.3. Рабочее место работников должно быть организовано таким способом, чтобы исключить просмотр документов с ПДн лицами, которые не допущены к ПДн.

9.4.4. Не разрешается хранение документов с ПДн на столах работников и в других, не предназначенных для этого местах.

9.4.5. Для обеспечения сохранности документов, содержащих ПДн, предотвращения их хищения, они подлежат хранению в условиях, исключающих несанкционированный к ним доступ.

9.5. Передача персональных данных

9.5.1. Предоставление персональных данных внутри компании

9.5.1.1. Под предоставлением ПДн понимаются действия, направленные на раскрытие ПДн определенному лицу/кругу лиц.

9.5.1.2. Доступ к ПДн субъекта имеют работники компании, которым ПДн необходимы в связи с исполнением ими трудовых обязанностей.

9.5.1.3. Работникам, допущенным к обработке ПДн, запрещено передавать, а также иным образом распространять ПДн, которые стали им известны, другим работникам компании, за исключением случаев, когда такая передача связана с исполнением должностных обязанностей.

9.5.1.4. Работники компании допускаются к обработке ПДн другого оператора только в связи с исполнением условий договора в рамках своих должностных обязанностей и в соответствии с установленным в компании порядком.

9.5.1.5. Процедура оформления доступа работника к ПДн включает в себя:

- ознакомление работника с настоящим положением, а также с другими локальными нормативными актами компании (приказами, распоряжениями и т.п.), регулирующими обработку ПДн субъектов;
- истребование с работника письменного обязательства о неразглашении персональных данных субъектов **(приложение Ж).**

9.5.1.6. Доступ к ПДн субъектов без специального разрешения имеют руководитель компании и иные лица, определенные распорядительным документом по компании (приказ/распоряжение).

9.5.1.7. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки. Данный принцип означает, что при направлении информации, содержащей ПДн, в другое подразделение или третьему лицу направлению подлежит объем информации необходимый получателю для исполнения своих функций.

9.5.1.8. Предоставление ПДн работника в пределах компании осуществляется на основании мотивированного письменного запроса руководителя структурного подразделения, которому необходимы ПДн работника в служебных целях.

9.5.1.9. ПДн работника могут передаваться в пределах компании с применением любого доступного и удобного установленного способа коммуникации работников (кольцевая почта, курьер, электронная почта и иное) с учетом ограничений, приведенных ниже.

9.5.1.10. При отправке бумажных документов, содержащих ПДн, по внутренней почте компании работники обязаны передаваемые документы вкладывать в бумажный конверт и ставить на нем пометку «Конфиденциально».

9.5.2. Предоставление персональных данных субъектов третьим лицам

9.5.2.1. Предоставление ПДн субъекта осуществляется только с письменного согласия субъекта, за исключением следующих случаев:

- передача данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством РФ на компанию функций, полномочий и обязанностей;
- передача данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве;
- передача данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн;
- передача данных необходима для защиты жизни, здоровья и иных жизненно важных интересов субъекта ПДн, если получение согласия невозможно;
- передача данных необходима для осуществления прав и законных интересов компании.

9.5.2.2. Письменное согласие на передачу ПДн третьей стороне включает в себя сведения, указанные в п.8.1 настоящего положения, а также наименование и адрес компании (третьего лица), получающей ПДн субъекта.

9.5.2.3. Компания в ходе своей деятельности осуществляет предоставление ПДн третьим лицам в целях исполнения договорных обязательств компании.

9.5.2.4. В договорах между компанией и третьими лицами в обязательном порядке определяется порядок предоставления ПДн. Договор с третьим лицом должен содержать раздел о конфиденциальности или отдельное соглашение о конфиденциальности передаваемой информации, включая ПДн. ПДн предоставляются третьей стороне в объеме, необходимом для достижения заявленных целей обработки.

9.5.2.5. Ответственность за соблюдение условий договоров в части обеспечения безопасности ПДн, а также контроля над исполнением этих условий принимающей стороной, возложена на структурное подразделение, взаимодействующее с третьими лицами.

9.5.2.6. Ответственность за соблюдение вышеуказанного порядка предоставления ПДн субъекта несет сотрудник компании, а также руководитель структурного подразделения, осуществляющего передачу ПДн субъекта третьим лицам.

9.5.2.7. ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда передача ПДн субъекта без его согласия допускается действующим законодательством.

9.5.2.8. Предоставление ПДн субъекта государственным органам, другим организациям и учреждениям осуществляется только по их письменному запросу в объеме, определенном предоставленными им полномочиями в соответствии с требованиями действующего законодательства.

9.5.2.9. Документы, содержащие персональные данные субъекта, могут быть отправлены почтовой связью. При этом обеспечивается их конфиденциальность.

9.5.2.10. При отправке почтовой связью комплектов документов, содержащих большие объемы ПДн, в целях обеспечения их конфиденциальности, применяется следующий порядок: документы, содержащие ПДн, вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

9.5.2.11. В ходе передачи данных по каналам информационно-телекоммуникационного обмена компания предпринимает меры по обеспечению защиты ПДн.

9.5.2.12. При передаче в рабочих целях файлов, содержащих ПДн, на внешние почтовые ящики (партнерам, контрагентам, государственным/правоохранительным органам, нотариальным конторам и т.п.), работники компании обязаны руководствоваться правилами, указанными ниже.

9.5.2.13. Допускается передача документов, содержащих ПДн, на официальные почтовые адреса[4] , перечисленных ниже получателей и не требует установки парольной защиты на архив:

- внутри компании или в общекорпоративной переписке;
- в государственные/правоохранительные органы, саморегулируемые организации (СРО), нотариальные конторы в связи с выполнением государственных и/или нотариальных функций по отношению к деятельности компании по мотивированному запросу;
- партнерам/контрагентам, на адрес почтового сервиса, указанного в качестве способа связи в тексте действующего договора выполнения работ/оказания услуг, соглашения о неразглашении информации и (или) соглашения о взаимодействии в сфере конфиденциальной информационной безопасности, исключительно в целях выполнения должностных обязанностей.

9.5.2.14. В целях обеспечения безопасности ПДн при передаче электронных документов с использованием средств защиты информации и каналов связи в компании устанавливаются следующие требования:

[4] Под официальным почтовым адресом понимается почтовый адрес, указанный в качестве способа связи в запросе от правоохранительных органов, органов государственной власти и управления, или в тексте действующего с партнерами\контрагентами договора на выполнение работ/оказание услуг и (или) соглашения о неразглашении конфиденциальной информации и (или) соглашения о взаимодействии в сфере информационной безопасности.

- передача ПДн совместному оператору ПДн или обработчику ПДн, возможна только при условии заключения соглашения о конфиденциальности;
- ПДн должны быть защищены и недоступны для третьих лиц, которые не являются совместными операторами или обработчиками с правами доступа к ПДн, в том числе ПДн должны быть недоступны для операторов связи (телекоммуникационных провайдеров), оказывающих услуги по передаче данных;
- при изменениях программного обеспечения или использовании технологий, которые влияют на состояние защищенности ПДн, до начала использования такого измененного программного обеспечения или технологий, третье лицо обязано письменно известить о произведенных изменениях контактное лицо со стороны компании, которое, в свою очередь, должно известить об этом Службу ИБ.

9.5.2.15. При передаче ПДн третьему лицу должны использоваться средства криптографической защиты каналов связи на основе технологий VPN, SSL и т. п., если применение таких средств выбрано в качестве меры защиты ПДн в проектной документации на систему защиты ПДн.

9.5.2.16. Организация взаимодействия при передаче ПДн при автоматизированной обработке производится путем утверждения доверенных каналов ПДн и обмена ключами/паролями в соответствии с документацией на средства защиты и распорядительными документами компании.

9.5.2.17. В случае необходимости осуществления трансграничной передачи ПДн подразделение, инициирующее такую передачу, до начала трансграничной передачи направляет запрос в Службу ИБ, с указанием следующих сведений:

- правовое основание и цель трансграничной передачи ПДн и дальнейшей обработки переданных ПДн;
- категории и перечень планируемых к передаче ПДн;
- категории субъектов ПДн, персональные данные которых планируется передавать;
- перечень иностранных государств, на территории которых планируется трансграничная передача ПДн.

9.5.2.18. Служба ИБ инициирует заседание Комиссии по организации обработки и защиты ПДн. Комиссия проводит анализ необходимости осуществления такой передачи и определяет перечень необходимых мероприятий в соответствии с требованиями Федерального закона «О персональных данных» (2.1.1). Решение Комиссии и сроки начала осуществления трансграничной передачи доводятся до сведения инициатора запроса.

9.5.3. Распространение персональных данных

9.5.3.1. Компания вправе распространять ПДн субъекта только при наличии его письменного согласия, оформленного отдельно от иных согласий субъекта в соответствии с требованиями действующего законодательства.

9.5.3.2. Разработка форм согласий на обработку ПДн, разрешенных субъектом ПДн для распространения, осуществляется Юридической службой по обращениям структурных подразделений в течение 10 рабочих дней с даты получения обращения. Такое обращение должно содержать следующую информацию:

- цель обработки ПДн;
- категорию субъекта ПДн (работник, контрагент или иное);
- категория и перечень ПДн, на распространение которых субъект ПДн дает согласие;
- сведения об информационных ресурсах оператора (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы), посредством которых будут осуществляться распространение ПДн;
- срок действия согласия.

9.5.3.3. Лицо, ответственное за взаимодействие с субъектом и/или инициирующее распространение ПДн, обязано обеспечить получение согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, от субъекта ПДн до начала распространения ПДн.

9.6. Поручение обработки персональных данных

9.6.1. Компания поручает обработку ПДн тем контрагентам, которые обеспечивают надлежащие гарантии применения соответствующих технических и организационных мер защиты таким образом, чтобы обработка отвечала требованиям российского законодательства и при необходимости GDPR и применимого законодательства иных стран.

9.6.2. Компания поручает обработку ПДн третьим лицам только с согласия субъекта ПДн или при наличии иного законного основания.

9.6.3. При передаче ПДн физическим лицам, выполняющим для компании работу по договору гражданско-правового характера (оказывающим услугу), требуется оформлять поручение обработки ПДн с такими лицами.

9.6.4. При поручении обработки ПДн третьим лицам в поручении на обработку ПДн в обязательном порядке должны быть определены:

- перечень действий (операций) с ПДн, которые будут совершаться лицом (перечень действий не должен противоречить целям и действиям, заявленным перед субъектом в договоре, согласии и т.д.);
- цели обработки (цели не должны противоречить целям, заявленным перед субъектом в договоре, в согласии и т.д.);
- обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке;
- обязанность такого лица по запросу оператора предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения требований оператора;
- перечень ПДн, поручаемых на обработку;
- требования к защите ПДн.

9.6.5. Типовая форма поручения приведена в **приложении И**.

9.6.6. При необходимости заключения поручения на обработку персональных данных инициатор направляет поручение на согласование посредством системы НЛМК@doc. В случае использования нетиповой формы поручения Юридическая служба оценивает возможность заключения поручения и проставляет в системе отметку о согласовании или мотивированном отказе в согласовании.

9.6.7. Передача ПДн третьему лицу до заключения соответствующего поручения запрещена.

9.6.8. Ответственность перед субъектом ПДн за действия третьего лица, которому поручена обработка ПДн, несет компания. Третье лицо, осуществляющее обработку ПДн по поручению компании, несет ответственность перед компанией.

9.6.9. Перечень третьих лиц, осуществляющих обработку ПДн по поручению Оператора (компании), размещен в общедоступном корпоративном источнике по ссылке https://nlmk.one/lp/ib/pd/ и доступен для ознакомления работников компании в любое удобное для них время. Служба ИБ актуализирует указанный перечень на основании данных информационной системы НЛМК@DOC.

9.7. Переносимость персональных данных

9.7.1. Компания обязана обеспечить возможность реализации права субъекта ПДн на переносимость данных (‘data portability’), когда выполняются следующие условия:

- обработка ПДн осуществляется на основании согласия субъекта ПДн; или обработка необходима для заключения или исполнения договора с субъектом;
- обработка осуществляется с использованием средств автоматизации.

9.7.2. Для информационных систем, обрабатывающих ПДн, в отношении которых должна обеспечиваться возможность портативности данных, должен быть предусмотрен функционал по извлечению ПДн в структурированном, общеупотребимом и машиночитаемом формате и передаче их третьему лицу (субъекту ПДн или другому оператору).

9.7.3. Взаимодействие с субъектом ПДн в целях реализации его права на переносимость ПДн осуществляется в порядке, определенном **приложением Е**.

9.8. Блокирование персональных данных

9.8.1. Обрабатываемые ПДн блокируются при выявлении недостоверности обрабатываемых сведений или неправомерных действий в отношении субъекта ПДн в следующих случаях:

- по требованию субъекта ПДн или его представителя;
- по требованию уполномоченного органа по защите прав субъектов;
- по результатам внутренних контрольных мероприятий в случае выявления неправомерной обработки ПДн;
- в случае отсутствия возможности уничтожения ПДн в установленные сроки до момента их уничтожения.

9.8.2. Блокирование осуществляется путем ограничения доступа пользователей к ПДн. Решение о блокировании ПДн принимает Ответственный за организацию обработки ПДн.

9.8.3. В случае, если причиной блокирования является неправомерная обработка ПДн, то после устранения выявленной неправомерной обработки блокирование ПДн снимают.

9.8.4. Решение о снятии блокирования ПДн субъекта принимает Ответственный за организацию обработки ПДн.

9.9. Уничтожение персональных данных

9.9.1. ПДн уничтожают в случае:

- выявления неправомерной обработки ПДн, в том числе, по обращению субъекта ПДн или его представителя либо запросу уполномоченного органа, если обеспечить

правомерность обработки ПДн невозможно в течение десяти рабочих дней с даты выявления неправомерной обработки персональных данных;

- требования субъекта ПДн, если его ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки в пределах 7 (семи) рабочих дней со дня представления таких сведений;
- отзыва субъектом ПДн согласия на обработку его ПДн, если сохранение ПДн более не требуется для целей их обработки или отсутствует иное основание для продолжения обработки ПДн в пределах сроков, указанных в п.8.3, с даты поступления указанного отзыва;
- достижения цели обработки ПДн или утраты необходимости в достижении этих целей - в течение 30 (тридцати) дней с даты достижения цели обработки ПДн;
- истечения сроков хранения ПДн, установленных законом;
- в иных, установленных законодательством случаях.

9.9.2. Оператор обеспечивает уничтожение ПДн (если за Оператора действует обработчик), кроме тех, которые Оператор обязан обрабатывать в соответствии с действующим законодательством Российской Федерации, в срок не более 30 (тридцати) дней с даты поступления указанного Заявления.

9.9.3. В случае невозможности уничтожить ПДн в течение установленного срока, Оператор блокирует ПДн или обеспечивает их блокирование (если за Оператора действует обработчик) и обеспечивает уничтожение ПДн в срок не более шести месяцев.

9.9.4. При возникновении вышеуказанного случая сотрудник, осуществляющий обработку ПДн, направляет в Службу ИБ следующую информацию:

- причину необходимости уничтожения ПДн;
- объем (примерное количество субъектов) ПДн, подлежащих уничтожению;
- содержание (категории) ПДн, подлежащих уничтожению;
- тип носителя (бумажный или электронный), где хранятся ПДн, подлежащие уничтожению, или наименование информационной системы, в которой обрабатываются персональные данные, подлежащие уничтожению.

9.9.5. При получении запроса Служба ИБ организует работу Комиссии по организации обработки и защиты ПДн с целью осуществления ею контроля за уничтожением ПДн.

9.9.6. В зависимости от типа носителя информации (бумажный или электронный) выделяют два способа уничтожения ПДн:

- физическое уничтожение носителя (уничтожение через шредерование, сжигание);
- уничтожение информации с электронного носителя и(или) из информационной системы ПДн.

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

9.9.8. После уничтожения персональных данных Комиссия составляет Акт об уничтожении персональных данных (далее Акт). Форма акта приведена в **приложении К**.

9.9.9. Подтверждением уничтожения ПДн в случае автоматизированной обработки ПДн является Акт и выгрузка из журнала регистрации событий в информационной системе ПДн (далее – выгрузка из журнала).

9.9.10. Выгрузка из журнала должна содержать:

- фамилию, имя, отчество (при наличии) субъекта или иную информацию, относящуюся к определенному физическом улицу, чьи ПДн были уничтожены;
- перечень категорий уничтоженных ПДн субъекта ПДн;
- наименование информационной системы ПДн, из которой были уничтожены ПДн;
- причину уничтожения ПДн;
- дату уничтожения ПДн.

9.9.11. Акт и (или) выгрузка из журнала подлежат хранению в Службе ИБ в течение 3 лет с момента уничтожения ПДн. В случае, если произведено уничтожение ПДн работника/ бывшего работника Оператора, копия Акта направляется в ООО «ЦКР» для хранения в личном деле субъекта ПДн.

9.10. Особенности неавтоматизированной обработки ПДн субъектов

9.10.1. Обработку ПДн без использования средств автоматизации осуществляют таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

9.10.2. При использовании типовых форм документов компании, характер информации в которых предполагает или допускает включение в них ПДн субъектов, от которых не получено согласие (далее типовая форма), соблюдаются следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес оператора, 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 оператором способов обработки ПДн;
- типовая форма предусматривает 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 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 исключает объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

9.10.3. При неавтоматизированной обработке ПДн на бумажных носителях не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы.

9.10.4. При хранении документов, содержащих ПДн, соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

9.11. Обработка данных между совместными операторами данных

9.11.1. Компания считается совместным оператором ПДн при выполнении следующих критериев:

- компания совместно с одним или несколькими третьими лицами определяет цели, состав и порядок обработки ПДн;
- компания и указанные третьи лица выступают в роли операторов ПДн.

9.11.2. Перед началом обработки компания и такие третьи лица должны определить, например, в форме соглашения, свои обязанности по соблюдению GDPR. В рамках такого соглашения должно быть определено, как минимум, следующее:

- область деятельности, в рамках которой будет осуществляться совместная обработка ПДн, и, где возможно, цели обработки и состав ПДн;
- распределение обязанностей и ответственности по реализации прав субъектов ПДн, и в отношении надзорных органов (например, назначение единого контактного лица для предоставления необходимой информации), включая распределение затрат;
- обязательства по взаимному содействию между совместными операторами (например, по предоставлению уведомлений о нарушении безопасности ПДн; ведению реестра обработки ПДн и проч.), включая механизмы обмена информацией;
- обязательства по возмещению потерь в отношении судебных решений, актов, соглашений, ответственности, ущерба, претензий, затрат, расходов и других издержек, понесенных в результате или в связи с нарушением обязательств, установленных GDPR и соответствующим соглашением.

10. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПДн ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА

10.1.1. Цель проведения внутреннего контроля состоит в определении соответствия порядка обработки ПДн работников компании и иных субъектов ПДн требованиям действующего законодательства и локальных нормативных актов компании.

10.1.2. Контроль соответствия обработки ПДн установленным требованиям разделяется на плановый и внеплановый.

10.1.3. Плановый контроль проводят в соответствии с утвержденным графиком проверок. Ответственным за ежегодное утверждение и составление графика проверок является Ответственный за организацию обработки ПДн.

10.1.4. Внеплановые проверки проводят в случае инцидента информационной безопасности, нарушения правил обработки и защиты ПДн, в случае информирования о предстоящей проверке регулирующими органами, в иных случаях по решению Ответственного за организацию обработки ПДн.

10.1.5. Внутренний контроль соответствия обработки ПДн требованиям законодательства и локальных нормативных актов компании осуществляет Комиссия по организации обработки и защите ПДн.

10.1.6. При проведении внутренней проверки Комиссия обязана в письменной форме уведомить руководителя проверяемого подразделения о дате и времени проведения проверки не менее чем за 3 рабочих дня до ее начала.

10.1.7. Результаты проверки оформляют в виде Акта произвольной формы, подписываемого всеми членами Комиссии, участвующими в проверке.

10.1.8. В акте указывают:

- нарушения и недостатки, выявленные в процессе проверки;
- причины выявленных несоответствий, возможные последствия;

- рекомендации по снижению рисков, устранению нарушений и недостатков;
- срок устранения выявленных замечаний.

11. ОБУЧЕНИЕ ПЕРСОНАЛА ПРАВИЛАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Обучение проводят с целью формирования и развития профессиональных знаний, навыков и умений работников компании, участвующих в обработке ПДн, в области обработки и защиты ПДн.

11.2. Обучение работников обработке и защите ПДн проводят одним из следующих способов:

- ознакомление работников с локальными нормативными актами компании, регулирующими обработку и защиту ПДн;
- проведение внутренних обучающих мероприятий в очном и дистанционном формате;
- изучение обучающих материалов в электронной форме с использованием корпоративных систем, ресурсов и материалов;
- участие в обучающих мероприятиях в сторонних организациях;
- рассылка информационных материалов по отдельным вопросам обработки и защиты ПДн.

11.3. Обучение сотрудников, участвующих в обработке ПДн, осуществляется в рамках Программы проведения обучения по информационной безопасности, утверждаемой Службой ИБ ежегодно.

11.4. Первичное ознакомление работников с локальными нормативными актами компании, регулирующими обработку и защиту ПДн, производит ООО «ЦКР» при трудоустройстве. В случае утверждения новых или внесения изменений в существующие локальные нормативные акты компании, регулирующие обработку и защиту ПДн, ознакомление проводят с помощью ИС НЛМК@doc.

12. ТРЕБОВАНИЯ К ХРАНЕНИЮ ДОКУМЕНТОВ И ЗАПИСЕЙ

12.1. Ответственный за организацию обработки ПДн обеспечивает хранение Перечня обрабатываемых ПДн и Реестра ПДн, подлежащих защите в соответствии с GDPR. Срок хранения данных документов 3 года.

12.2. Сроки хранения ПДн в компании определены в Перечне обрабатываемых ПДн и Реестре персональных данных, подлежащих защите в соответствии с GDPR.

13. ОТВЕТСТВЕННОСТЬ

13.1. Ответственность за выполнение требований настоящего положения возложена на руководителей и работников компании в рамках своих полномочий в процессе обработки и защиты ПДн.

13.2. Ответственность за контроль исполнения требований настоящего положения возложена на Ответственного за организацию обработки ПДн.

РАЗРАБОТАНО

Начальник управления

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Подлинник электронного документа хранится в системе электронного документооборота НЛМК@DOC

Идентификатор подписи **7850a90e-0f6d-41bd-8d7e-289b2fe1ac88**
Подписант **Моломин В.В.**
Должность **Начальник управления**
Дата подписания **13.08.2026 16:12 МСК**

В.В. Моломин

ПРИЛОЖЕНИЕ А
(справочное)
Термины и определения

А.1. В настоящем положении применены следующие термины с соответствующими определениями в соответствии с **Единым корпоративным глоссарием**:

А.1.1. **Компания:** хозяйственное общество, которое является резидентом РФ, и в которой НЛМК прямо и/или косвенно распоряжается акциями/долями.

А.1.2. **Функциональное направление (ФН)**: функция, управление которой осуществляется с прямым подчинением руководителя функции Президенту (Председателю Правления).

А.2. Дополнительно в настоящем положении применены следующие термины с соответствующими определениями:

А.2.1. **Автоматизированная обработка персональных данных:** обработка ПДн с помощью средств вычислительной техники.

А.2.2. **Блокирование персональных данных**: временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

А.2.3. **Внутренняя типовая форма:** документ, состав данных и порядок обработки которого не установлен законодательством Российской Федерации, и использующийся во внутренних бизнес-процессах компании.

А.2.4. **Информационная система персональных данных:** совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

А.2.5. **Инцидент:** любое непредвиденное или нежелательное событие, которое нарушает (или может нарушить) безопасность ПДн.

А.2.6. **Обезличивание персональных данных:** действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту персональных данных.

А.2.7. **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 ПДн.

А.2.8. **Обработчик (‘processor'):** лицо, обрабатывающее ПДн исключительно на основе инструкций Оператора.

A.2.9. **Ограничение обработки:** маркировка сохраненных ПДн в целях ограничения их обработки в будущем.

A.2.10. **Оператор (‘controller’):** (1) 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. (2) Лицо, определяющее самостоятельно или совместно с другими лицами цели, состав и порядок обработки ПДн, которое несет ответственность за соблюдение требований к обработке и защите ПДн.

ПРИЛОЖЕНИЕ А
(окончание)

A.2.11. **Переносимость персональных данных (right to data portability):** право субъекта ПДн на безвозмездное предоставление Оператором другому Оператору электронной копии ПДн субъекта по требованию самого субъекта ПДн.

A.2.12. **Персональные данные:** любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

A.2.13. **Предоставление персональных данных:** действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

A.2.14. **Прекращение обработки (обеспечение прекращения обработки) персональных данных:** действия по уничтожению или, если это невозможно выполнить в течение установленного срока, блокированию персональных данных.

A.2.15. **Профилирование (‘profiling’):** любая форма автоматизированной обработки ПДн, в рамках которой ПДн используются для оценки персональных особенностей физических лиц, в частности, рабочей эффективности, экономической ситуации, здоровья, индивидуальных предпочтений, интересов, надежности, поведения, местоположения или передвижений.

A.2.16. **Процесс обработки персональных данных:** бизнес-процесс компании, в рамках которого осуществляется обработка ПДн.

A.2.17. **Распространение персональных данных:** действия, направленные на раскрытие ПДн неопределенному кругу лиц.

A.2.18. **Реестр персональных данных:** реестр ПДн, подлежащих защите в соответствии с GDPR, который ведется Оператором.

A.2.19. **Совместный оператор (‘joint controller’):** оператор, который совместно с другими операторами персональных данных, определяет цели, состав и порядок обработки персональных данных.

A.2.20. **Согласие на обработку:** свободно данное, конкретное, информированное и недвусмысленное изъявление воли субъекта данных, посредством которого субъект соглашается на обработку относящихся к нему ПДн.

A.2.21. **Трансграничная передача персональных данных:** передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

A.2.22. **Третье лицо:** физическое или юридическое лицо, органы государственной власти, агентство или иной орган, отличный от субъекта данных, оператора (контролера) или

лиц, которые уполномочены проводить обработку ПДн под непосредственным руководством оператора или обработчика.

А.2.23. **Уничтожение персональных данных:** действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

А.2.24. **Уполномоченный орган по защите прав субъектов персональных данных:** федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки ПДн требованиям законодательства РФ в области ПДн.

ПРИЛОЖЕНИЕ Б
(обязательное)
Порядок назначения в компании ответственных лиц, их задачи, функции и права

Б.1. Ответственный за организацию обработки ПДн

Б.1.1. Общие положения

Б.1.1.1. Ответственный за организацию обработки ПДн назначается приказом руководителя компании.

Б.1.1.2. При назначении учитываются полномочия, компетенции и личностные качества ответственного, призванные позволить ему надлежащим образом и в полном объеме реализовать свои права и выполнять свои обязанности.

Б.1.1.3. Ответственный за организацию обработки ПДн обязан соблюдать тайну или конфиденциальность в отношении выполняемых им задач в соответствии с законодательством РФ.

Б.1.1.4. Ответственный за организацию обработки ПДн при выполнении своих задач должным образом учитывает риск, связанный с обработкой, с учетом характера, сферы применения, контекста и целей обработки.

Б.1.2. Основные задачи и функции

Б.1.2.1. Ответственный за организацию обработки ПДн выполняет следующие задачи и функции:

- своевременно составляет и направляет в уполномоченный орган по защите прав субъектов ПДн уведомление о намерении компании осуществлять обработку ПДн / информационное письмо о внесении изменений в реестр операторов ПДн;
- в случае изменения сведений в указанных выше уведомлении/ информационном письме, в установленные сроки уведомляет об этих изменениях уполномоченный орган по защите прав субъектов ПДн;
- совместно с Юридической службой осуществляет взаимодействие от лица компании с уполномоченным органом по защите прав субъектов ПДн и другими государственными органами в случаях, предусмотренных законодательством РФ в области ПДн и GDPR;
- организовывает работу по получению согласия субъектов ПДн на обработку ПДн в случаях, предусмотренных законодательством РФ в области ПДн и GDPR;
- организовывает экспертизу локальных нормативных актов компании, регулирующих порядок обработки ПДн, договоров с третьими лицами в части конфиденциальности передаваемых ПДн, поручений на обработку ПДн;
- организовывает работу по проведению обучения персонала в вопросах обработки и защиты ПДн;
- организовывает осуществление внутренней проверки за соблюдением компанией и её работниками требований локальных нормативных актов компании, регулирующих порядок обработки ПДн, а также законодательства РФ в области обработки ПДн и GDPR;

ПРИЛОЖЕНИЕ Б
(продолжение)

- организовывает доведение до сведения работников компании положений законодательства РФ, GDPR и локальных нормативных актов компании по вопросам организации обработки ПДн;
- организовывает прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществляет контроль над приемом и обработкой таких обращений и запросов;
- осуществляет иные задачи и функции, указанные в настоящем положении.

Б.1.2.2. Ответственный за организацию обработки ПДн должен знать:

- требования действующего законодательства РФ в области ПДн и GDPR;
- принципы организации системы защиты персональных данных в соответствии с требованиями законодательства РФ в области ПДн и GDPR;
- бизнес-процессы, существующие в компании, связанные с обработкой ПДн;
- характер взаимодействия подразделений в процессе обработки ПДн, а также порядок обработки ПДн в них.

Б.1.3. Права

Б.1.3.1. Ответственный за организацию обработки ПДн в целях решения возложенных на него задач имеет право:

- требовать от работников компании выполнения требований локальных нормативных актов компании, а также действующего законодательства РФ в области обработки ПДн и GDPR;
- давать обязательные для исполнения поручения всем службам компании в целях обеспечения выполнения задач и функций Ответственного за организацию обработки ПДн в рамках их компетенции;
- требовать от должностных лиц выполнения обязанностей, возложенных на них настоящим положением, действующим законодательством РФ в области обработки ПДн и GDPR;
- запрашивать и получать от работников компании информацию для исполнения своих прав и обязанностей;
- инициировать изменения в бизнес-процессы, связанные с обработкой ПДн, если это обусловлено необходимостью обеспечения соответствия законодательству РФ в области обработки ПДн и GDPR;
- выступать с ходатайством к руководителю компании/ФН/структурного подразделения о поощрении или наложении взысканий на работников в связи с исполнением ими обязанностей, связанных с обработкой ПДн.

Б.2. Ответственный за обеспечение безопасности ПДн

Б.2.1. Общие положения

Б.2.1.1. Ответственный за обеспечение безопасности ПДн назначается при наличии требований по обеспечению соответствующего уровня защищенности ПДн при их обработке в ИСПДн из числа работников компании, связанных с обеспечением информационной безопасности.

ПРИЛОЖЕНИЕ Б
(продолжение)

Б.2.1.2. В своей деятельности Ответственный за обеспечение безопасности ПДн руководствуется действующим законодательством РФ, GDPR, локальными нормативными актами компании.

Б.2.2. Основные задачи и функции

Б.2.2.1. Ответственный за обеспечение безопасности ПДн выполняет следующие задачи и функции:

- общее руководство и контроль над обеспечением безопасности ПДн в компании;
- определение требований к защите ПДн при их обработке в ИСПДн;
- согласование нормативной документации компании по защите ПДн;
- согласование технической документации на СЗПДн;
- взаимодействие с контролирующими органами по вопросам обеспечения безопасности ПДн и координация работников компании при проведении плановых и внеплановых проверок, а также при обработке их запросов;
- разработка инструментов, мероприятий по защите ПДн при их обработке;
- проведение инструктажей работников по правилам обеспечения безопасности ПДн при их обработке;
- организация построения и поддержания в актуальном состоянии системы защиты ПДн как комплекса организационных и технических мер защиты, в том числе с привлечением специалистов иных подразделений;
- формирование планов проведения контрольных мероприятий по защите ПДн (в т.ч. мероприятий по оценке эффективности мер защиты ПДн), представляющих собой комплекс мероприятий внутреннего контроля для проверки выполнения правил обеспечения безопасности ПДн и организация их выполнения;
- оценка потенциального вреда субъектам ПДн в случае нарушения безопасности ПДн, оценка актуальности угроз безопасности ПДн, при их обработке в ИСПДн;
- оценка необходимости привлечения сторонних организаций (подрядчиков) для обслуживания, настойки и ремонта средств защиты ПДн;
- информирование руководства компании о состоянии СЗПДн, о планируемых мероприятиях, нацеленных на обеспечение безопасности ПДн, а также о результатах проведенных мероприятий;
- участие в процессе реагирования и расследования инцидентов ИБ, связанных с обеспечением безопасности ПДн;
- оценка необходимости корректировки нормативной документации по обеспечению безопасности ПДн, модернизации технических средств СЗПДн по результатам проведения контрольных мероприятий (в т.ч. оценки эффективности мер защиты ПДн), оценки актуальности угроз безопасности ПДн, расследования инцидентов ИБ, связанных с обеспечением безопасности ПДн.

ПРИЛОЖЕНИЕ Б
(окончание)

Б.2.2.2. Ответственный за обеспечение безопасности ПДн должен знать:

- требования действующего законодательства РФ в области ПДн и GDPR;
- общие принципы организации СЗПДн в соответствии с требованиями законодательства в области ПДн;
- бизнес-процессы, существующие в компании, в которых обрабатываются ПДн;
- процессы обеспечения и управления ИБ;
- характер взаимодействия подразделений компании, а также порядок обработки ПДн в них;
- структуру ИС компании, категории и объем защищаемых ПДн, категории пользователей, обрабатывающих ПДн и их права доступа к ПДн;
- структуру СЗПДн, применяемое нормативное обеспечение, используемые технические средства защиты информации.

Б.2.3. Права

Б.2.3.1. Ответственный за обеспечение безопасности ПДн имеет право:

- требовать от работников компании выполнения требований локальных нормативных актов, а также действующего законодательства РФ в области обеспечения безопасности ПДн и GDPR;
- требовать от работников компании выполнения своих обязанностей, связанных с построением и поддержанием в актуальном состоянии системы защиты персональных данных, невыполнение которых может повлечь к нарушениям требований законодательства РФ в области обеспечения безопасности ПДн и GDPR;
- запрашивать и получать от работников компании информацию для исполнения своих прав и обязанностей;
- выступать с ходатайством к руководству компании о внесении изменений в процессы ИБ, а также в ИСПДн и СЗПДн, если это обусловлено необходимостью обеспечения соответствия законодательству РФ в области обеспечения безопасности ПДн и GDPR;
- выступать с ходатайством к руководству компании о проведении необходимых организационных и технических мероприятий в рамках выполнения требований законодательства РФ и GDPR в области обеспечения безопасности ПДн;
- выступать с ходатайством к руководству компании о привлечении внешних организаций для выполнения работ по защите ПДн;
- выступать с ходатайством к руководителю компании/ФН/структурного подразделения о поощрении или наложении взысканий на работников в связи с исполнением ими обязанностей, связанных с защитой ПДн.

ПРИЛОЖЕНИЕ В
(обязательное)
Матрица разграничения ответственности по процессам обработки и защиты ПДн

Таблица В.1 - Исполняемые роли

В - Роль "Владелец»	участник бизнес-процесса, который отвечает за результаты/конечный продукт бизнес-процесса: разрабатывает методологию, определяет уровень качества, осуществляет планирование, организацию, контроль и совершенствование процесса
С - Роль «Согласующий»	участник бизнес-процесса, который согласует/утверждает решение или действие, возникающее по результатам выполнения бизнес-процесса, а также может предоставлять консультационную и/или методологическую поддержку
И - Роль «Исполнитель»	участник бизнес-процесса, который выполняет необходимые действия для получения результата исполнения процесса и несет ответственность за их результат
Ин - Роль «Информируемый»	участник бизнес-процесса, который получает данные в процессе и/или по результатам выполнения описываемого бизнес-процесса
В С, И В С, И В	наличие больше одной маркировки роли обозначает выполнение разных ролей в рамках одного указанного процесса

Таблица В.2 - Матрица разграничения ответственности по процессам обработки и защиты ПДн

Процессы обработки и защиты ПДн	**Служба ИБ**	**Юридическая служба**	**Комиссия по организации обработки и защиты ПДн**	**ООО «ЦКР»**	**HR БП**
1. Сбор и анализ информации о порядке и способах обработки ПДн	В И С	И С	С	-	-
2. Определение состава и границ ИСПДн	В И С	-	С	-	-
3. Определение набора мер по обеспечению безопасности ПДн при их обработке в ИСПДн на основании установленных уровней защищенности с учетом актуальных угроз безопасности ПДн и используемых информационных технологий	В И С	-	-	-	-
4. Оценка эффективности реализованных мер по обеспечению безопасности ПДн при их обработке в ИСПДн	В И С	-	Ин	-	-
5. Разработка/актуализация локальных нормативных актов компании в области обеспечения безопасности ПДн (Политика информационной безопасности, Положение об обеспечении безопасности ПДн и пр.)	В И	С	Ин	Ин	-
6. Разработка/актуализация локальных нормативных актов компании, регламентирующих общие требования к обработке ПДн с учетом требований законодательства и лучших практик в области обработки ПДн (Политика в области обработки и защиты ПДн, Положение об обработке ПДн и пр.) включая разработку форм согласий на обработку ПДн для каждого нового вида обработки, форм согласий на обработку ПДн, разрешенных субъектом ПДн для распространения, формы Поручения на обработку ПДн третьим лицам и иных форм, на которые имеется ссылка в настоящем положении	В И	И С	Ин	Ин	-

ПРИЛОЖЕНИЕ В
(окончание)

7. Ознакомление работников компании с локальными нормативными актами в области ПДн в части их касающейся	В И	С	-	И	-
8. Сбор согласий работников компании на обработку ПДн	В	С	-	И	И
9. Проведение оценки вреда, который может быть причинен субъектам ПДн	В И	И	И С	-	-
10. Координация процесса Поручения обработки ПДн третьему лицу. Включает оценку возможности поручения такой обработки конкретному лицу, объема и целей поручения, контроль процесса подписания Поручения, включая проверку проекта Поручения	В	И С	-	-	-
11. Внедрение принципа запланированной защищённости данных на стадии проектирования бизнес-процесса в котором осуществляется обработка ПДн, за исключением случаев разработки ИСПДн. Проводится анализ наличия правовых оснований для обработки ПДн, соответствие цели обработки объему собираемых данных с учетом изменений как во внутреннем, так и во внешнем контексте. (комментарий: Юридическая служба осуществляет оценку защищенности и правомерности обработки данных существующих бизнес –процессов или появление новых только в том случае, когда не разрабатывается новая ИСПДн или вносятся изменения в текущую. Эти исключения относятся к функционалу Службы ИБ)	В И	И С	-	-	-
12. Проведение внутреннего контроля соответствия обработки ПДн требованиям законодательства и локальным нормативным актам компании	В И	И	И С	-	-
13. Обучение работников компании правилам обработки ПДн	В И	И	-	-	-
14. Поддержание в актуальном состоянии Уведомления об обработке ПДн в реестре операторов ПДн Роскомнадзор	В И С	С	Ин	-	-
15. Поддержание в актуальном состоянии Перечня обрабатываемых ПДн и Реестра ПДн, подлежащих защите в соответствии с GDPR	В И	С	-	-	-
16. Рассмотрение вопросов о необходимости осуществления трансграничной передачи ПДн	В И	И	И С	-	-
17. Проведение собеседования с субъектом ПДн (работником компании) для разъяснения юридических последствий отзыва согласия на обработку ПДн	И Ин	В И Ин	-	-	И
18. Передача в ООО «ЦКР» акта о проведении собеседования о разъяснении юридических последствий отзыва согласия и заявления об отзыве согласия для хранения в личном деле	-	-	-	Ин	И
19. Уничтожение ПДн работника компании, заявившего об отзыве согласия на обработку ПДн	Ин С	В И С	С	И	-
20. Уничтожение ПДн субъекта, не являющегося работником компании, заявившего об отзыве согласия на обработку ПДн	И С	В И С	С	-	-
21. Подготовка ответа субъекту ПДн, заявившему об отзыве согласия на обработку ПДн	С Ин	В И	-	-	-
22. Направление ответа субъекту ПДн (работнику компании), заявившему об отзыве согласия на обработку ПДн, и копии ответа в ООО «ЦКР» для хранения в личном деле	-	Ин	-	Ин	И

ПРИЛОЖЕНИЕ Г
(обязательное)
Форма согласия на обработку персональных данных для работников компании

Согласие
на обработку персональных данных

Я, _____
(фамилия, имя, отчество полностью)
дата рождения _____,
(год, месяц, число)
данные основного документа, удостоверяющего личность:
вид документа _____ серия _____ номер_____
дата выдачи _____ орган, выдавший документ _____
_____
адрес регистрации _____,
действуя своей волей и в своем интересе, даю согласие организации *Название компании*, (далее Оператор),
наименование Оператора: *Название компании*
адрес Оператора: *Юридический адрес компании*
на обработку моих персональных данных в целях осуществления:

- трудовых отношений согласно трудовому договору и Трудовому Кодексу РФ;
- договорных отношений в рамках заключенных с контрагентами договоров, а также подготовки к заключению и реализации договоров;
- социальных программ, связанных с действующими работниками, бывшими работниками и другими лицами, в том числе, с ветеранами, в целях обеспечения льгот и гарантий;
- совместных с учебными заведениями программ в области подготовки кадров, в том числе, в отношении работников организации и других лиц;
- пропуска на территорию организации;
- деятельности, связанной с учетом интересов акционеров общества;
- единой политики Группы НЛМК по основным направлениям деятельности (включая, но не ограничиваясь в области кадров, антикоррупционной политики, политики в области охраны труда и промышленной безопасности);
- политики сотрудничества с органами государственной власти и местными органами власти;
- других видов деятельности в рамках законодательства РФ, с обязательным выполнением требований законодательства РФ в области персональных данных.

К персональным данным, на обработку которых я даю согласие, относятся фамилия, имя, отчество, сведения о дате и месте рождения, об образовании, о владении иностранными языками, о научной деятельности, о трудовой деятельности; сведения автобиографии, об участии в военных действиях и ликвидации чрезвычайных ситуаций, о пребывании за границей, о поощрениях, взысканиях и наградах; о семейном положении, составе и членах семьи, паспортные данные, ИНН, СНИЛС, контактные данные (телефоны, электронная почта); сведения адресного характера, сведения о производственной деятельности; данные для обеспечения льгот и гарантий, фотографическое изображение, видеоизображение, данные аттестаций и характеристик, сведения о профессиональном образовании, профессиональной переподготовке, сведения о доходах, об обязательствах имущественного характера; о прохождении медицинских профилактических осмотров, о частичной или временной нетрудоспособности.

ПРИЛОЖЕНИЕ Г
(окончание)

Предоставляемое мною согласие на обработку персональных данных распространяется на все способы обработки, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, уничтожение, как с использованием, так и без использования средств автоматизации.

Даю согласие считать общедоступными мои следующие персональные данные в любых сочетаниях между собой: фамилия, имя, отчество, пол, дата рождения, данные об образовании, место работы, период работы, должность, профессия, данные об обучении и профессиональном развитии, данные о наградах и поощрениях, данные об участии в социальных программах организации, фотографическое изображение, видеоизображение, контактные данные (телефоны, электронная почта). Предоставляю Оператору право осуществлять с моими общедоступными персональными данными все вышеуказанные способы обработки, действия (операции), а также передачу неопределенному кругу лиц путем размещения в общедоступных корпоративных источниках.

Даю согласие на передачу моих персональных данных третьим лицам с целью осуществления третьими лицами их обработки в интересах *Название компании*, на основании договора, содержащего поручение обработки и обеспечения безопасности и конфиденциальности персональных данных. Я ознакомлен и согласен с тем, что перечень третьих лиц, осуществляющих обработку моих персональных данных по поручению Оператора, размещен в общедоступном корпоративном источнике по следующей ссылке https://nlmk.one/lp/ib/pd/ и доступен для ознакомления в любое удобное для меня время. Даю согласие на изменение перечня третьих лиц по усмотрению Оператора.

Даю согласие на обработку моих персональных данных после расторжения трудовых отношений по вопросам, возникшим в период действия трудового договора до полного их разрешения.

Настоящее согласие вступает в силу с момента предоставления мною персональных данных и действует вплоть до отзыва мной согласия в установленном порядке.

Я предупрежден, что персональные данные могут быть использованы лишь в целях, для которых они сообщены.

Я ознакомлен с тем, что отзыв данного согласия может быть осуществлен в любой момент времени посредством направления в адрес Оператора, подписанного мною или моим законным представителем письменного уведомления по почте заказным письмом с уведомлением о вручении или вручением лично под расписку представителю кадровой службы Оператора.

Я осознаю, что в случае отзыва мной согласия в рамках трудовых отношений с Оператором дальнейшая обработка персональных данных будет продолжаться в целях исполнения обязательств по Трудовому договору и в соответствии с Трудовым кодексом РФ.

Я ознакомлен с тем, что мои персональные данные будут храниться оператором в течение 75 лет после расторжения трудового договора в соответствии с Архивным законодательством РФ.

Согласие составлено _____
(число, месяц, год)

Подпись дающего согласие _____

_____
(фамилия, имя, отчество прописью полностью)

ПРИЛОЖЕНИЕ Д
(обязательное)
Акт разъяснения субъекту персональных данных юридических последствий отзыва согласия на обработку персональных данных

В рамках рассмотрения отзыва согласия на обработку персональных данных, поступившего ___.___. 202_г. от _____,
(фамилия, имя, отчество субъекта персональных данных или его представителя)

было проведено собеседование для разъяснения субъекту персональных данных юридических последствий отзыва согласия на обработку персональных данных и/или его информирования о наличии иных законных оснований для обработки его персональных данных, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", в соответствии с которыми Оператор вправе продолжить обработку персональных данных без его согласия.

На собеседовании присутствовали представители Оператора:

- …;
- …;
- …

Субъект персональных данных и/или его представитель на собеседовании:

☐ присутствовал, ему были разъяснены юридические последствия отзыва согласия на обработку персональных данных, он подтвердил отзыв согласия;

☐ присутствовал, ему были разъяснены юридические последствия отзыва согласия на обработку персональных данных, он отменил отзыв согласия;

☐ присутствовал, был проинформирован о наличии иных законных оснований для обработки его персональных данных, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", в соответствии с которыми Оператор вправе продолжить обработку персональных данных без его согласия;

☐ не присутствовал (осознано отказался участвовать или не явился), тем самым, подтвердил отзыв согласия обработку персональных данных вне зависимости от разъяснения юридических последствий отзыва согласия и/или информирования о наличии иных законных оснований для обработки его персональных данных, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", в соответствии с которыми Оператор вправе продолжить обработку персональных данных без его согласия.

«___» _____ 202_г.

Подписи присутствующих представителей Оператора:

_____ / И.О. Фамилия;

_____ / И.О. Фамилия;

_____ / И.О. Фамилия.

ПРИЛОЖЕНИЕ Е
(обязательное)
Порядок взаимодействия с субъектами персональных данных

Е.1. Назначение документа

Е.1.1. Настоящий документ описывает порядок действий при поступлении запросов и обращений субъектов ПДн или их законных представителей с целью реализации законных прав субъектов ПДн в отношении ПДн в соответствии с действующим законодательством РФ и ЕС.

Е.2. Запросы и обращения от субъектов, находящихся на территории РФ

Субъекты ПДн или их законные представители вправе направлять запросы и обращения с целью реализации следующих прав:

- права на получение информации об обработке ПДн, в том числе содержащей:
  - подтверждение факта обработки ПДн компанией;
  - правовые основания и цели обработки ПДн;
  - способы обработки ПДн;
  - наименование и место нахождения компании, сведения о лицах (за исключением работников компании), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с компанией или на основании федерального закона;
  - обрабатываемые ПДн субъекта, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
  - сроки обработки ПДн, в том числе сроки их хранения;
  - порядок осуществления субъектом ПДн прав, предусмотренных ФЗ «О персональных данных»;
  - информацию об осуществленной или о предполагаемой трансграничной передаче данных;
  - наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению компании, если обработка поручена или будет поручена такому лицу;
  - иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

Субъект ПДн вправе обратиться повторно к компании или направить ему повторный запрос в целях получения указанных выше сведений, и ознакомления с такими ПДн не ранее чем через **тридцать дней** после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн.

Данное правило применяется в случае если компания на первый запрос в полном объеме предоставила субъекту ПДн запрашиваемую информацию.

- права на уточнение его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- права на отзыв согласия на обработку ПДн.

Запросы и обращения могут быть направлены лично субъектом данных; лицом, уполномоченным направить Запрос от лица субъекта в форме:

ПРИЛОЖЕНИЕ Е
(продолжение)

- бумажного документа;
- электронного документа, который должен быть подписан электронной подписью в соответствии с законодательством РФ.

Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя; сведения о дате его выдачи и выдавшем его органе;
- сведения, подтверждающие участие субъекта ПДн в отношениях с компанией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн компанией;
- подпись субъекта ПДн или его представителя.

При необходимости от субъекта или его законного представителя запрашивается дополнительная информация.

В случае отказа в предоставлении указанной выше информации, компания в письменной форме направляет мотивированный отказ в срок, не превышающий 30 дней со дня обращения или с даты получения запроса.

В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, компания вносит необходимые изменения.

В пределах сроков, указанных в п. 8.3 Положения, со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, компания уничтожает такие ПДн, уведомляет субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах, принимает разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

При наличии возможности ответ должен быть дан в той же форме, в которой был получен запрос.

Ответ на запрос должен содержать минимум необходимой информации, напрямую связанной с запросом. При оформлении ответа необходимо использовать четкие и простые формулировки.

Е.3. Запросы и обращения от субъектов, находящихся на территории ЕС

Субъекты ПДн вправе обратиться к компании с целью реализации следующих прав:

- право на доступ (подтверждение факта обработки его ПДн, предоставление сведений о такой обработке);
- право на исправление (исправление ошибочных или неактуальных данных и дополнение неполных данных);
- право на удаление данных «право на забвение» (удаление своих ПДн в случае, если у компании отсутствуют достаточные основания на их обработку);
- право на ограничение обработки (ограничение обработки своих данных);

ПРИЛОЖЕНИЕ Е
(окончание)

- право на переносимость своих данных (предоставление обрабатываемых ПДн в структурированном, общеупотребимом и машиночитаемом формате и, где технически возможно, передача ПДн другой организации);
- право выразить несогласие с обработкой ПДн (несогласие с обработкой относящихся к нему ПДн без необходимости демонстрировать убедительные законные основания такого несогласия);
- право отзыва согласия (отзыв согласия на обработку его ПДн, в случаях, когда обработка ведется на основании согласия субъекта).

Запросы и обращения могут быть направлены в форме:

- бумажного документа;
- электронного документа;
- заполнения формы запроса, размещенной на сайте компании.

Запрос может быть направлен:

- лично субъектом данных;
- лицом, уполномоченным направить запрос от лица субъекта ПДн, например, лицо, назначенное судом или другим компетентным органом действовать от лица субъекта ПДн, согласно применимому законодательству;
- лицом, должным образом уполномоченным субъектом данных подписать и (или) подать запрос от лица субъекта ПДн (например, на основании должным образом оформленного согласия субъекта ПДн или доверенности).

Компания сообщает субъекту ПДн или его законному представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также представляет возможность ознакомления с этими ПДн в течении 10 рабочих дней с момента получения запроса.

Срок обработки запроса может быть продлен не более чем на 5 рабочих дней по мотивированному уведомлению, которое направляется в адрес субъекта ПДн. Обработка запроса субъекта ПДн и подготовка ответа должны выполнятся без взимания платы с субъекта. Допускается взимание платы только в том случае, если компания может продемонстрировать избыточность и необоснованность запроса, в частности, из-за его регулярного характера (например, если запрашиваемые данные и действия сотрудников компании те же, что и в запросе, который был обработан компанией ранее). Общая стоимость выполнения процедур по выполнению запроса на перенос данных не должна приниматься во внимание при определении избыточности запроса.

Если компания не выступает в роли Оператора (контролера) в отношении ПДн, являющихся предметом запроса, или не обрабатывает такие ПДн, в адрес Заявителя направляется ответ о том, что запрос не может быть выполнен, с объяснением причин отказа.

При наличии возможности ответ должен быть дан в той же форме, в которой был получен запрос.

Ответ на запрос должен содержать минимум необходимой информации, напрямую связанной с запросом. При оформлении ответа необходимо использовать четкие и простые формулировки.

ПРИЛОЖЕНИЕ Ж
(обязательное)
Форма Обязательства о неразглашении персональных данных субъектов

ОБЯЗАТЕЛЬСТВО

о неразглашении персональных данных субъектов

г. _____ «___» _____ 20__ г.

Я, _____
(ФИО)

_____ табельный номер _____
(наименование структурного подразделения)

обязуюсь:

1. не сообщать третьей стороне персональные данные субъектов, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей, за исключением случаев, предусмотренных действующим законодательством РФ;

2. соблюдать порядок обработки и передачи персональных данных субъектов, установленный Положением об обработке персональных данных в компании, а также другими локальными нормативными актами (приказами, распоряжениями, инструкциями и т.п.), регулирующими обработку и защиту персональных данных в компании;

3. в случае попытки третьих лиц получить от меня персональные данные субъектов сообщать об этом непосредственному руководителю, а также Ответственному за организацию обработки персональных данных в компании;

4. обеспечивать сохранность документов, содержащих персональные данные субъектов, ключей от хранилищ и сейфов (металлических шкафов);

5. об утрате или недостаче носителей персональных данных субъектов, ключей доступа, ключей от хранилищ и сейфов или о других фактах, которые могут привести к утечке персональных данных субъектов, немедленно сообщать должностному лицу структурного подразделения, ответственному за обработку персональных данных;

До моего сведения доведены с разъяснениями соответствующие положения по обеспечению сохранности персональных данных субъектов, установленные законодательством и локальными нормативными актами компании.

Мне известно, что нарушение этих положений может повлечь гражданскую, уголовную, административную, дисциплинарную ответственность в соответствии с действующим законодательством Российской Федерации.

« _____ » _____ 20 ____ г. _____ _____
(ФИО работника) (подпись)

Экземпляр обязательства получил(а): _____ _____
(ФИО) (подпись)

ПРИЛОЖЕНИЕ И
(обязательное)
Форма поручения обработки персональных данных

Поручение на обработку персональных данных №__

___ _____ 20__ года

_____именуемое в дальнейшем «Исполнитель», в лице_____, действующей на основании _____, с одной стороны, и _____именуемое в дальнейшем «Заказчик», в лице_____, действующего на основании_____, с другой стороны, руководствуясь частью 3 статьи 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» заключили настоящий договор-поручение на осуществление другим лицом обработки персональных данных (далее поручение) о нижеследующем:

1. ПРЕДМЕТ ПОРУЧЕНИЯ

1.1. По настоящему поручению Заказчик, с согласия субъектов персональных данных, передает Исполнителю персональные данные сотрудников Заказчика, а также иных лиц, а Исполнитель обязуется по поручению Заказчика осуществлять обработку указанных персональных данных до момента расторжения настоящего Поручения на обработку персональных данных либо до момента достижения цели обработки персональных данных.

1.2. Исполнитель осуществляет обработку персональных данных сотрудников Заказчика, а также иных лиц, персональные данные которых используются Заказчиком, в следующих формах: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.3. Исполнитель вправе самостоятельно и за свой счет привлекать к обработке персональных данных в порядке перепоручения третьи лица (субисполнителей), с которыми у Исполнителя заключены соответствующие договоры для достижения целей, указанных п.2.1 настоящего Поручения, при соблюдении следующих условий:

1.3.1. Исполнитель информирует Заказчика о принятом решении привлечения или замене текущего субисполнителя по обработке персональных данных. Информация направляется Ответственным за организацию обработки персональных данных Исполнителя Ответственному за организацию обработки персональных данных Заказчика по электронной почте. В сообщении указывается наименование и адрес субисполнителя, а также сведения о том, какие персональные данные каких субъектов и в каких целях переданы субисполнителю.

1.3.2. Исполнитель оценивает достаточность применяемых субисполнителем средств защиты и конфиденциальности данных предъявляемых Заказчиком.

1.3.3. Исполнитель несет ответственность перед Заказчиком за любые нарушения, допущенные субисполнителем при обработке данных.

ПРИЛОЖЕНИЕ И
(продолжение)

2. ЦЕЛЬ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПЕРЕДАВАЕМЫХ ДЛЯ ОБРАБОТКИ

2.1. Обработка персональных данных сотрудников Заказчика, а также иных субъектов персональных данных, персональные данные которых обрабатываются Заказчиком, осуществляется с целью _____.

2.2. Перечень персональных данных, передаваемых Заказчиком, приведен в Приложении 1 к настоящему Поручению.

2.3. Персональные данные, передаваемые Заказчиком, обрабатываются автоматизированным способом (в информационных системах персональных данных Исполнителя) и/или неавтоматизированным способом (на бумажных носителях).

3. ОБЯЗАТЕЛЬСТВА СТОРОН

3.1. Исполнитель обязан:

3.1.1. Соблюдать принципы и правила обработки персональных данных, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

3.1.2. Сохранять конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также выполнять требования к защите обрабатываемых персональных данных в соответствии с действующим законодательством Российской Федерации.

3.1.3. Использовать для записи и хранения персональных данных базы данных на территории Российской Федерации.

3.1.4. Принимать надлежащие технические и организационные меры по обеспечению безопасности в соответствии с требованиями статьи 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»:

- 1) применять организационные меры по обеспечению безопасности персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает заявленный Заказчиком уровень защищенности персональных данных;
- 2) организовать защиту технических средств, на которых обрабатываются персональные данные, полученные от Заказчика, в соответствии с Приказом ФСТЭК от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- 3) обеспечить уничтожение персональных данных по обращению Заказчика в случае принятия им решения о прекращении обработки персональных данных и (или) отзыве поручения на обработку персональных данных.
- Данные меры включают в себя:

– назначение ответственного за организацию обработки персональных данных;
– издание документа, определяющий политику в отношении обработки и защиты персональных данных и локальных актов по вопросам обработки и защиты персональных данных;
– обеспечение раздельного хранения персональных данных (материальных носителей) обработка которых осуществляется в различных целях;

ПРИЛОЖЕНИЕ И
(продолжение)

- обеспечение сохранности персональных данных и исключение несанкционированного доступа к ним;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение средств защиты информации, при необходимости прошедших в установленном порядке процедуру оценки соответствия;
- проведение оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- выявление фактов несанкционированного доступа к персональным данным с принятием соответствующих мер по снижению ущерба от несанкционированного доступа и недопущению дальнейшего несанкционированного доступа;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивать регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- применение мер по обеспечению безопасности ПДн, направленных на нейтрализацию актуальных угроз безопасности ПДн, таких как:
  - идентификация и аутентификация субъектов доступа и объектов доступа;
  - управление доступом субъектов доступа к объектам доступа;
  - защита машинных носителей информации;
  - регистрация событий безопасности;
  - обеспечение антивирусной защиты;
  - контроль (анализ) защищенности информации;
  - защита среды виртуализации;
  - защита технических средств;
  - защита информационной системы, ее средств, систем связи и передачи данных;
  - управление конфигурацией информационной системы и системы защиты ПДн;
- осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных;
- соблюдение требований федеральных законов и иных нормативных правовых актов в сфере обработки и защиты персональных данных.

3.1.5. Письменно уведомлять Заказчика о возникновении угрозы безопасности персональных данных, переданных Заказчиком Исполнителю.

ПРИЛОЖЕНИЕ И
(продолжение)

3.1.6. Совершать какие-либо действия в отношении персональных данных, которые он обрабатывает от имени Заказчика, исключительно в соответствии с указаниями Заказчика.

3.1.7. Письменно уведомлять Заказчика о блокировании (приостановке) функционирования или доступа к ресурсам Заказчика с указанием причин и сроков.

3.1.8. Незамедлительно письменно уведомлять Заказчика в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных.

3.1.9. По письменному запросу Заказчика предоставлять отчетную документацию и материалы, подтверждающие выполнение исполнение обязательств по настоящему поручению в течение 10 (десяти) рабочих дней с даты поступления запроса.

3.1.10. Предоставлять доступ к персональным данным, полученным от Заказчика, третьим лицам только после уведомления Заказчика в порядке предусмотренным п.1.3.1.

3.1.11. Исполнять иные обязательства, предусмотренные действующим законодательством.

3.2. Исполнитель имеет право:

3.2.1. Запрашивать у Заказчика информацию, необходимую для выполнения поручения в рамках настоящего договора.

3.2.2. Обеспечивать непосредственный доступ третьих лиц к ресурсам Заказчика без разрешения Заказчика только по требованиям, в целях и в случаях, предусмотренных действующим законодательством Российской Федерации с последующим своевременным уведомлением Заказчика по электронной почте, в срок не более 3 (трёх) рабочих дней с даты предоставления такого доступа.

3.3. Заказчик обязан:

3.3.1. Принять и (или) обеспечить на уровне информационной системы персональных данных Заказчика принятие технических и иных мер, установленных законодательством, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.3.2. Реагировать на запросы субъектов персональных данных, касающиеся обработки их персональных данных в информационных системах Заказчика, а также Исполнителя, обрабатывающего персональные данные по поручению Заказчика.

3.3.3. Сообщать Исполнителю обо всех изменениях в составе персональных данных, переданных для обработки.

3.4. Заказчик имеет право:

3.4.1. Получать полную информацию о порядке защиты персональных данных у Исполнителя.

3.4.2. Определять требования к порядку защиты персональных данных, соблюдая требования действующего законодательства, предписания уполномоченных государственных органов, требования действующих договоров с Исполнителем.

ПРИЛОЖЕНИЕ И
(окончание)

3.4.3. Потребовать уничтожения данных в случае принятия решения о прекращении обработки персональных данных и (или) отзыве поручения у Исполнителя.

3.4.4. Затребовать отчет, указанный в пункте 3.1.8 настоящего Поручения не чаще 1 раза в течение календарного года.

4. СРОК ДЕЙСТВИЯ, ПОРЯДОК ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ ПОРУЧЕНИЯ

4.1. Настоящее Поручение вступает в силу с момента его подписания обеими сторонами и действует до момента его расторжения.

4.2. Изменения, дополнения и приложения к настоящему Поручению оформляются в письменном виде, являются неотъемлемыми частями настоящего Поручения и вступают в силу с момента их подписания обеими сторонами.

5. ИНЫЕ УСЛОВИЯ

5.1. Вопросы, не урегулированные настоящим Поручением, разрешаются в соответствии с действующим законодательством Российской Федерации.

6. АДРЕСА, РЕКВИЗИТЫ, ПОДПИСИ СТОРОН

Приложение № 1
к Поручению на обработку персональных данных

Перечень персональных данных, передаваемых Заказчиком Исполнителю в рамках Поручения на обработку персональных данных

<Могут быть указаны:

- *персональные данные конкретных субъектов ПДн*
  или
- *перечень обрабатываемых персональных данных>*

Заказчик **Исполнитель**

ПРИЛОЖЕНИЕ К
(обязательное)
Форма акта об уничтожении персональных данных

УТВЕРЖДАЮ

_____
Председатель комиссии

_____ _____
подпись расшифровка подписи

« _____ » _____ _____
число месяц год

АКТ №_____

Об уничтожении персональных данных

«__» _____20__г.

Комиссия в составе председателя _____, членов комиссии _____, созданная на основании приказа/распоряжения от «___»_____ 20__г. № _____, руководствуясь Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", составила акт о том, что Оператором персональных данных _____ (наименование, адрес) и/или лицом, осуществляющим обработку персональных данных по поручению оператора _____ (наименование или ФИО, адрес) если обработка была поручена такому лицу, произведено уничтожение персональных данных в следующем объеме:

№ п/п	ФИО субъекта персональных данных	Содержание (категории) уничтоженных персональных данных	Тип / наименование носителя, объем уничтоженных персональных данных (кол-во листов)	Наименование информационной системы персональных данных

Перечисленные персональные данные уничтожены по причине _____.

Перечисленные персональные данные уничтожены путем _____.

Данный акт подлежит хранению в течение 3 лет с момента уничтожения персональных данных.

Председатель комиссии: Должность _____ / Фамилия И.О.

Члены комиссии: Должность _____ / Фамилия И.О.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ К ПОЛОЖЕНИЮ

Номер изменения	Дата введения в действие	Перечень измененных пунктов

ЛИСТ РЕДАКЦИЙ ПОЛОЖЕНИЯ

Ред. №	Наименование документа	Дата утверждения	Дата введения в действие	Реквизиты распорядительного документа
1	П LG-162-0006-2019 «Положение об обработке и защите персональных данных»	01.02.2019	01.02.2019	Приказ от 06.02.2019 №52
2	П LG-162-0006-2020 «Положение об обработке персональных данных»	15.06.2021	15.06.2021	Приказ от 11.06.2021 №53-341-П-ОД
3	П LG-162-0006-2023 «Положение об обработке персональных данных»	03.11.2023	03.11.2021	Приказ от 30.10.2023 №53-155-П-ОД