Унифицированная форма № Т1
Утверждена постановлением Госкомстата
России от 05.01.04 .№1

	Код
Форма по ОКУД	0301000
по ОКПО	

Федеральное государственное бюджетное учреждение науки Институт океанологии им. П.П. Ширшова Российской академии наук (ИО РАН)

Номер документа	Дата
157/17	23.10.2023

ПРИКАЗ

Об утверждении локальных нормативных актов о защите персональных данных

В целях актуализации локальных нормативных актов в отношении обработки персональных данных и в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение о персональных данных (Приложение № 1).
2. Утвердить и ввести в действие Политику в отношении обработки персональных данных (Приложение № 2).
3. Утвердить и ввести в действие Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных требованиям законодательства Российской Федерации (Приложение № 3).
4. Утвердить форму письменного согласия на обработку персональных данных (приложение № 4).
5. Утвердить форму обязательство о неразглашении конфиденциальной информации (персональных данных), не содержащих сведений, составляющих государственную тайну (Приложение № 5).
6. Приказ ИО РАН от 17.11.2021 № 136 «Об утверждении Положения о персональных данных ИО РАН» признать утратившими силу.
7. Контроль за исполнением настоящего приказа возлагаю на себя.

Врио директора В.П. Шевченко

Приложение № 1
к приказу от 23.10.2023 № 157 П

Федеральное государственное бюджетное учреждение науки
ИНСТИТУТ ОКЕАНОЛОГИИ им. П.П. ШИРШОВА РОССИЙСКОЙ АКАДЕМИИ НАУК (ИО РАН)

УТВЕРЖДЕНО
приказом директора
от 23.10.2023 № 157 П

ПОЛОЖЕНИЕ
о персональных данных

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) и определяет порядок обращения с персональными данными работников Федерального государственного бюджетного учреждения науки Института океанологии им. П.П. Ширшова Российской академии наук (далее – ИО РАН).

1.2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов ИО РАН и его работников в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные.

1.3. В Положении устанавливаются:

- цель, порядок и условия обработки персональных данных;
- категории субъектов, персональные данные которых обрабатываются, категории (перечни) обрабатываемых персональных данных, способы, сроки их обработки и хранения, порядок уничтожения таких данных при достижении целей обработки или при наступлении иных законных оснований;
- положения, касающиеся защиты персональных данных, процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных, на устранение последствий таких нарушений.

1.4. Сведения о персональных данных работников относятся к числу конфиденциальной информации. Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания;
- по истечении 75 лет срока их хранения;
- в других случаях, предусмотренных федеральными законами.

2. Основные понятия. Состав персональных данных работников

2.1. Для целей настоящего Положения используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных

данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

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

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия конкретного лица или иного законного основания;

общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в

соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. Согласно Положению персональные данные обрабатываются с целью применения и исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ними отношений, в том числе:

– при содействии в трудоустройстве;

– в ведении кадрового и бухгалтерского учета;

– в содействии работникам в получении образования и продвижении по службе;

– в оформлении награждений и поощрений;

– в предоставлении со стороны ИО РАН установленных законодательством условий труда, гарантий и компенсаций;

– в заполнении и передаче в уполномоченные органы требуемых форм отчетности;

– в обеспечении личной безопасности работников и сохранности имущества;

– в осуществлении контроля за количеством и качеством выполняемой работы.

2.3. Информация, представляемая работником при поступлении на работу в ИО РАН, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации (далее – ТК РФ) лицо, поступающее на работу, предъявляет:

– паспорт или иной документ, удостоверяющий личность;

– трудовую книжку, за исключением случаев, когда договор заключается впервые при сохранении бумажкой версии трудовой книжки, или копию трудовой книжки при поступлении на работу на условиях совместительства, либо выписку из электронной трудовой книжки;

– страховой номер индивидуального лицевого счета (СНИЛС);

– документы воинского учета - для лиц, подлежащих воинскому учету;

– документ об образовании и (или) квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

– свидетельство о присвоении ИНН (при его наличии у работника);

– справку, выданную органами МВД России, о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, к которой в соответствии с ТК РФ или иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию).

2.4. При оформлении работника отделом кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

– общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

– сведения о воинском учете;

– данные о приеме на работу;

– сведения об аттестации;
– сведения о повышенной квалификации;
– сведения о профессиональной переподготовке;
– сведения о наградах (поощрениях), почетных званиях;
– сведения об отпусках;
– сведения о социальных гарантиях;
– сведения о месте регистрации и о контактных телефонах.

2.5. В отделе кадров ИО РАН создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.5.1. Документы, содержащие персональные данные работников:

– комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;
– комплекс материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;
– подлинники и копии приказов (распоряжений) по кадрам; личные дела и трудовые книжки;
– дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестаций работников; дела, содержащие материалы внутренних расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); доверенности на работников, содержащие сведения о паспортных данных и адрес места жительства работника;
– подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Института, руководителям структурных подразделений;
– копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

2.5.2. Документация по организации работы структурных подразделений:

– положения о структурных подразделениях;
– должностные инструкции работников;
– приказы, распоряжения, указания руководства Института;
– документы планирования, учета, анализа и отчетности по вопросам кадровой работы.

2.6. Документация, подлежащая длительному хранению, передается на хранение в Архив ИО РАН.

2.7. ИО РАН не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством Российской Федерации.

3. Обработка персональных данных работников

3.1. Источником информации обо всех персональных данных работника является непосредственно работник. Если персональные данные возможно получить только у третьей стороны, то работник должен быть заранее в письменной форме уведомлен об этом и от него должно быть получено письменное согласие. ИО РАН обязан сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа работника дать письменное согласие на их

получение.

3.2. Обработка персональных данных работников ИО РАН возможна только с их согласия либо без их согласия в следующих случаях:

– персональные данные являются общедоступными;

– персональные данные относятся к состоянию здоровья работника, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

– по требованию полномочных государственных органов - в случаях, предусмотренных федеральным законом.

3.3. Обработка персональных данных в ИО РАН выполняется следующими способами:

– неавтоматизированная обработка персональных данных;

– автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;

– смешанная обработка персональных данных.

3.4. Обработка биометрических персональных данных допускается только при наличии письменного согласия субъекта персональных данных. Исключение составляют ситуации, предусмотренные ч. 2 ст. 11 Закона о персональных данных.

3.5. ИО РАН вправе обрабатывать персональные данные работников только с их письменного согласия.

3.6. Письменное согласие работника на обработку своих персональных данных должно включать в себя:

– фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

– срок, в течение которого действует согласие, а также порядок его отзыва.

3.7. Согласие работника не требуется в следующих случаях:

– обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия ИО РАН;

– обработка персональных данных в целях исполнения трудового договора;

– обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

3.8. Работник ИО РАН представляет в отдел кадров достоверные сведения о себе.

Отдел кадров проверяет достоверность сведений.

3.9. В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина руководитель ИО РАН и его законные, полномочные представители при обработке персональных данных работника должны выполнять следующие общие требования:

3.9.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов или иных правовых актов, содействия работникам в трудоустройстве, получении образования и профессиональном продвижении, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.9.2. При определении объема и содержания, обрабатываемых персональных данных, ИО РАН должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

3.9.3. При принятии решений, затрагивающих интересы работника, ИО РАН не имеет права основываться на персональных данных, полученных о нем исключительно в результате их автоматизированной обработки или электронного получения.

3.9.4. Защита персональных данных работника от неправомерного их использования, утраты обеспечивается ИО РАН за счет его средств в порядке, установленном федеральным законом.

3.9.5. Работники и их представители должны быть ознакомлены под расписку с документами ИО РАН, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.9.6. Во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен.

4. Передача персональных данных работников

4.1. При передаче персональных данных работника ИО РАН должен соблюдать следующие требования:

4.1.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.

4.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

4.1.3. Предупредить лиц, получивших персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

4.1.4. Осуществлять передачу персональных данных работников в пределах Института в соответствии с настоящим Положением.

4.1.5. Разрешать доступ к персональным данным работников только специально

уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

4.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

4.1.7. Передавать персональные данные работника его законным, полномочным представителям в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции.

4.2.Персональные данные работников обрабатываются и хранятся в отделе кадров ИО РАН и филиалов.

4.3. При получении персональных данных не от работника (за исключением случаев, если персональные данные являются общедоступными) ИО РАН до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

– наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
– цель обработки персональных данных и ее правовое основание;
– предполагаемые пользователи персональных данных;
– установленные федеральными законами права субъекта персональных данных.

5. Доступ к персональным данным работников

5.1.Право доступа к персональным данным работников имеют:

– руководитель ИО РАН и руководители филиалов;
– работники кадровых служб ИО РАН и филиалов;
– работники бухгалтерии ИО РАН и филиалов;
– работники отдела информационных технологий ИО РАН и специалистов по информационным технологиям филиалов (информация о рабочем месте, данные о приеме на работу, контактные телефоны работников);
– работники юридического отдела ИО РАН и филиалов (информация о фактическом месте проживания и контактные телефоны работников);
– работники секретариата ИО РАН и филиалов (информация о фактическом месте проживания и контактные телефоны работников);
– начальник первого отдела (доступ к персональным данным работников в ходе плановых проверок);
– руководители структурных подразделений по направлению деятельности ИО РАН и филиалов (доступ к персональным данным только работников своего подразделения).

5.2. Работник ИО РАН (филиалов) имеет право:

5.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копии любой записи, содержащей его персональные данные.

5.2.2. Требовать от ИО РАН (филиалов) уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для ИО РАН (филиалам) персональных данных.

5.2.3. Получать от ИО РАН (филиалов):

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

5.2.4. Требовать извещения ИО РАН (филиалами) всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия ИО РАН (филиалов) при обработке и защите его персональных данных.

5.3. Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения начальника отдела кадров и филиалов.

5.4. Передача информации третьей стороне возможна только при письменном согласии работников.

6. Порядок блокирования и уничтожения персональных данных

6.1. ИО РАН (филиалы) блокирует персональные данные в порядке и на условиях, предусмотренных законодательством в области персональных данных.

6.2. При достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей персональные данные уничтожаются либо обезличиваются. Исключение может предусматривать федеральный закон.

6.3. Незаконно полученные персональные данные или те, которые не являются необходимыми для цели обработки, уничтожаются в течение семи рабочих дней со дня представления субъектом персональных данных (его представителем) подтверждающих сведений.

6.4. Персональные данные, обработка которых прекращена из-за ее неправомерности и правомерность обработки которых невозможно обеспечить, уничтожаются в течение 10 рабочих дней с даты выявления факта неправомерной обработки.

6.5. Персональные данные уничтожаются в течение 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иным соглашением между ним и ИО РАН, либо если ИО РАН не вправе обрабатывать персональные данные без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6.6. При достижении максимальных сроков хранения документов, содержащих персональные данные, персональные данные уничтожаются в течение 30 дней.

6.7. Персональные данные уничтожаются (если их сохранение не требуется для целей обработки персональных данных) в течение 30 дней с даты поступления отзыва субъектом персональных данных согласия на их обработку. Иное может предусматривать договор, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иное соглашение между ним и ИО РАН. Кроме того, персональные данные уничтожаются в указанный срок, если ИО РАН не вправе

обрабатывать их без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6.8. Отбор материальных носителей (документы, жесткие диски, флеш-накопители и т.п.) и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению, осуществляют подразделения ИО РАН, обрабатывающие персональные данные.

6.9. Уничтожение персональных данных осуществляет комиссия, утвержденная директором.

6.10. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

6.11. Персональные данные на бумажных носителях уничтожаются с использованием шредера. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

6.12. Комиссия подтверждает уничтожение персональных данных согласно Требованиям к подтверждению уничтожения персональных данных, утвержденным приказом Роскомнадзора от 28.10.2022 № 179, а именно:

– актом об уничтожении персональных данных - если данные обрабатываются без использования средств автоматизации;

– актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных - если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, которые должны содержаться в указанных документах, утверждаются приказом ИО РАН.

7. Защита персональных данных. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений

7.1. Без письменного согласия субъекта персональных данных ИО РАН не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

7.2. Запрещено раскрывать и распространять персональные данные субъектов персональных данных по телефону.

7.3. С целью защиты персональных данных в ИО РАН приказами ИО РАН назначаются (утверждаются):

– работник, ответственный за организацию обработки персональных данных;

– перечень должностей, при замещении которых обрабатываются персональные данные;

– перечень персональных данных, к которым имеют доступ работники, занимающие должности, предусматривающие обработку персональных данных;

– порядок доступа в помещения, в которых ведется обработка персональных

данных;

– порядок передачи персональных данных в пределах ИО РАН;

– форма согласия на обработку персональных данных, форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения;

– порядок защиты персональных данных при их обработке в информационных системах персональных данных;

– порядок проведения внутренних расследований, проверок;

– иные локальные нормативные акты, принятые в соответствии с требованиями законодательства в области персональных данных.

7.4. Работники, которые занимают должности, предусматривающие обработку персональных данных, допускаются к ней после подписания обязательства об их неразглашении.

7.5. Материальные носители персональных данных хранятся в шкафах, запирающихся на ключ. Помещения ИО РАН, в которых они размещаются, оборудуются запирающими устройствами.

7.6. Доступ к персональной информации, содержащейся в информационных системах ИО РАН, осуществляется по индивидуальным паролям.

7.7. В ИО РАН используется сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

7.8. Работники ИО РАН, обрабатывающие персональные данные, периодически проходят обучение требованиям законодательства в области персональных данных.

7.9. В должностные инструкции работников ИО РАН, обрабатывающих персональные данные, включаются, в частности, положения о необходимости сообщать о любых случаях несанкционированного доступа к персональным данным.

7.10. В ИО РАН проводятся внутренние расследования в следующих ситуациях:

– при неправомерной или случайной передаче (предоставлении, распространении, доступе) персональных данных, повлекшей нарушение прав субъектов персональных данных;

– в иных случаях, предусмотренных законодательством в области персональных данных.

7.11. Работник, ответственный за организацию обработки персональных данных, осуществляет внутренний контроль:

– за соблюдением работниками, уполномоченными на обработку персональных данных, требований законодательства в области персональных данных, локальных нормативных актов;

– соответствием указанных актов требованиям законодательства в области персональных данных. Внутренний контроль проходит в виде внутренних проверок.

7.12. Внутренние плановые проверки осуществляются на основании ежегодного плана, который утверждается директором.

7.13. Внутренние внеплановые проверки осуществляются по решению работника, ответственного за организацию обработки персональных данных. Основанием для них служит информация о нарушении законодательства в области персональных данных, поступившая в устном или письменном виде.

7.14. По итогам внутренней проверки оформляется служебная записка на имя

директора. Если выявлены нарушения, в документе приводится перечень мероприятий по их устранению и соответствующие сроки.

7.15. Внутреннее расследование проводится, если выявлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных (далее - инцидент).

7.16. В случае инцидента ИО РАН в течение 24 часов уведомляет Роскомнадзор:

– об инциденте;

– о его предполагаемых причинах и вреде, причиненном правам субъекта (нескольким субъектам) персональных данных;

– о принятых мерах по устранению последствий инцидента;

– о представителе ИО РАН, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

7.17. При направлении уведомления нужно руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными приказом Роскомнадзора от 14.11.2022 № 187.

7.18. В течение 72 часов ИО РАН обязано сделать следующее:

– уведомить Роскомнадзор о результатах внутреннего расследования;

– предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии).

7.19. При направлении уведомления также необходимо руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными приказом Роскомнадзора от 14.11.2022 № 187.

7.20. В случае предоставления субъектом персональных данных (его представителем) подтвержденной информации о том, что персональные данные являются неполными, неточными или неактуальными, в них вносятся изменения в течение семи рабочих дней. ИО РАН уведомляет в письменном виде субъекта персональных данных (его представителя) о внесенных изменениях и сообщает (по электронной почте) о них третьим лицам, которым были переданы персональные данные.

7.21. ИО РАН уведомляет субъекта персональных данных (его представителя) об устранении нарушений в части неправомерной обработки персональных данных. Уведомляется также Роскомнадзор, если он направил обращение субъекта персональных данных (его представителя) либо сам сделал запрос.

7.22. В случае уничтожения персональных данных, которые обрабатывались неправомерно, уведомление направляется в соответствии с настоящим Положением.

7.23. В случае уничтожения персональных данных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки, ИО РАН уведомляет субъекта персональных данных (его представителя) о принятых мерах в письменном виде. ИО РАН уведомляет по электронной почте также третьих лиц, которым были переданы такие персональные данные.

8. Ответственность за нарушение норм, регулирующих обработку персональных данных

8.1. Работники ИО РАН, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к их защите, установленных Законом о персональных данных, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

9. Заключительные положения

9.1. Настоящее положение, а также все изменения и дополнения к нему утверждаются и вводятся в действие приказом директора ИО РАН.

9.2. Настоящее положение действует до его замены новым.

Приложение № 2
к приказу от 23.10.2023 № 157 П

Федеральное государственное бюджетное учреждение науки
ИНСТИТУТ ОКЕАНОЛОГИИ им. П.П. ШИРШОВА РОССИЙСКОЙ АКАДЕМИИ НАУК (ИО РАН)

УТВЕРЖДЕНО
приказом директора
от 23.10.2023 № 157 П

ПОЛИТИКА
в отношении обработки персональных данных

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) Федерального государственного бюджетного учреждения науки Института океанологии им. П.П. Ширшова Российской академии наук (далее – Институт) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иными нормативными правовыми актами в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных.

1.2. Институт является оператором персональных данных как государственное юридическое лицо, самостоятельно организующее и осуществляющее обработку таких данных, а также определяющее цели их обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.3. На Институт, согласно ст. 22 Закона о персональных данных как на оператора персональных данных распространяется исключение по обязанности уведомлять уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) о своем намерении осуществлять обработку персональных данных, как организации осуществляющей обработку персональных данных в соответствии с трудовым законодательством. В связи с этим Институт не включается в реестр операторов персональных данных.

1.4. Политика действует в отношении всех персональных данных, которые обрабатывает Институт.

1.5. Политика распространяется на отношения в области обработки персональных данных, возникшие у Института как до, так и после утверждения настоящей Политики.

1.6. Институт и его филиалы имеют право:

1.7.1. самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми

актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;

1.7.2. поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Института, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;

1.7.3. в случае отзыва субъектом персональных данных согласия на обработку персональных данных Институт вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных.

1.7. Институт и его филиалы обязаны:

1) организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;

2) отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;

3) сообщать в уполномоченный орган по защите прав субъектов персональных данных (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)) по запросу этого органа необходимую информацию в течение 10 рабочих дней с даты получения такого запроса. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Институту необходимо направить в Роскомнадзор мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации;

4) в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование его о компьютерных инцидентах, которые повлекли неправомерную передачу (предоставление, распространение, доступ) персональных данных.

1.8. Основные права субъекта персональных данных. Субъект персональных данных имеет право:

1) получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Институтом в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;

2) требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

3) дать предварительное согласие на обработку персональных данных в целях

продвижения на рынке товаров, работ и услуг;

4) обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Института при обработке его персональных данных.

1.8. Контроль за исполнением требований настоящей Политики осуществляется уполномоченным лицом, ответственным за организацию обработки персональных данных у Института.

1.9. Ответственность за нарушение требований законодательства Российской Федерации и локальных нормативных актов Института в сфере обработки и защиты персональных данных определяется в соответствии с законодательством Российской Федерации.

2. Основные понятия

2.1. Для целей настоящей Политике используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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

обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

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

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия конкретного лица или иного законного основания;

общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

3. Цели сбора персональных данных

3.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.2. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.3. Обработка Институтом персональных данных осуществляется в следующих целях:

– осуществление своей деятельности в соответствии с уставом Института, в том числе заключение и исполнение договоров с контрагентами;

– исполнение трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, в том числе: содействие работникам в трудоустройстве, получении образования и продвижении по службе, привлечение и отбор кандидатов на работу у Института, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества, ведение кадрового учета, заполнение и передача в уполномоченные органы требуемых форм отчетности, организация постановки на индивидуальный (персонифицированный) учет работников в системах обязательного пенсионного страхования и обязательного социального страхования;

– осуществление пропускного режима.

3.4. Обработка персональных данных работников может осуществляться

исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

4.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки Политики. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.2. Институт может обрабатывать персональные данные следующих категорий субъектов персональных данных.

4.2.1. Кандидаты для приема на работу к Институту - для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, осуществления пропускного режима:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата и место рождения;
- контактные данные;
- сведения об образовании, опыте работы, квалификации;
- иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

4.2.2. Работники и бывшие работники Института - для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, осуществления пропускного режима:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата и место рождения;
- изображение (фотография);
- паспортные данные;
- адрес регистрации по месту жительства;
- адрес фактического проживания;
- контактные данные;
- индивидуальный номер налогоплательщика;
- страховой номер индивидуального лицевого счета (СНИЛС);
- сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;
- семейное положение, наличие детей, родственные связи;
- сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий;
- данные о регистрации брака;
- сведения о воинском учете;
- сведения об инвалидности;
- сведения об удержании алиментов;

– сведения о доходе с предыдущего места работы;

– иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

4.2.3. Заказчики и контрагенты Института (физические лица) - для целей осуществления своей деятельности в соответствии с уставом Института, осуществления пропускного режима:

– фамилия, имя, отчество;

– дата и место рождения;

– паспортные данные;

– адрес регистрации по месту жительства;

– контактные данные;

– замещаемая должность;

– индивидуальный номер налогоплательщика;

– номер расчетного счета;

– иные персональные данные, предоставляемые клиентами и контрагентами (физическими лицами), необходимые для заключения и исполнения договоров.

4.2.4. Представители (работники) клиентов и контрагентов Института (юридических лиц) - для целей осуществления своей деятельности в соответствии с уставом Института, осуществления пропускного режима:

– фамилия, имя, отчество;

– паспортные данные;

– контактные данные;

– замещаемая должность;

– иные персональные данные, предоставляемые представителями (работниками) клиентов и контрагентов, необходимые для заключения и исполнения договоров.

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

5. Порядок и условия обработки персональных данных

5.1. Обработка персональных данных осуществляется Институтом в соответствии с требованиями законодательства Российской Федерации.

5.2. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

5.3. Институт осуществляет обработку персональных данных для каждой цели их обработки следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

5.4. К обработке персональных данных допускаются работники Института, в должностные обязанности которых входит обработка персональных данных.

5.5. Обработка персональных данных для каждой цели обработки осуществляется путем:

- получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных;
- внесения персональных данных в журналы, реестры и информационные системы Института;
- использования иных способов обработки персональных данных.

5.6. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, утверждены приказом Роскомнадзора от 24.02.2021 № 18.

5.7. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Социальный фонд России и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

5.8. Институт принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

- определяет угрозы безопасности персональных данных при их обработке;
- принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;
- назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Института;
- создает необходимые условия для работы с персональными данными;
- организует учет документов, содержащих персональные данные;
- организует работу с информационными системами, в которых обрабатываются персональные данные;
- хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;
- организует обучение работников Института, осуществляющих обработку персональных данных.

5.9. Институт осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требует каждая цель обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

5.9.1. Персональные данные на бумажных носителях хранятся в Институте в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в Российской Федерации (Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Перечень типовых

управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. приказом Росархива от 20.12.2019 № 236)).

5.9.2. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

5.10. Институт прекращает обработку персональных данных в следующих случаях:

- выявлен факт их неправомерной обработки. Срок - в течение трех рабочих дней с даты выявления;
- достигнута цель их обработки;
- истек срок действия или отозвано согласие субъекта персональных данных на обработку указанных данных, когда по Закону о персональных данных обработка этих данных допускается только с согласия.

5.11. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку Институт прекращает обработку этих данных, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- Институт не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;
- иное не предусмотрено другим соглашением между Институтом и субъектом персональных данных.

5.12. При обращении субъекта персональных данных к Институту с требованием о прекращении обработки персональных данных в срок, не превышающий 10 рабочих дней с даты получения Институтом соответствующего требования, обработка персональных данных прекращается, за исключением случаев, предусмотренных Законом о персональных данных. Указанный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Институту необходимо направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока.

5.13. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Институт обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

6. Актуализация, исправление, удаление, уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

6.1. Подтверждение факта обработки персональных данных Институтом, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Институтом субъекту персональных данных или его представителю в течение 10 рабочих дней с момента

обращения либо получения запроса субъекта персональных данных или его представителя. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Институту следует направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации.

В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

Запрос должен содержать:

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

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Институт предоставляет сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

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

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

6.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Институт осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Институт на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.3. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Институт осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента

такого обращения или получения запроса.

6.4. При выявлении Институтом, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Институт:

- в течение 24 часов - уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Институтом на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;
- в течение 72 часов - уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

6.5. Порядок уничтожения персональных данных Институтом.

6.5.1. Условия и сроки уничтожения персональных данных Институтом:

- достижение цели обработки персональных данных либо утрата необходимости достигать эту цель - в течение 30 дней;
- достижение максимальных сроков хранения документов, содержащих персональные данные, - в течение 30 дней;
- предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки, - в течение семи рабочих дней;
- отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, - в течение 30 дней.

6.5.2. При достижении цели обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- Институт не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;
- иное не предусмотрено другим соглашением между Институтом и субъектом персональных данных.

6.5.3. Уничтожение персональных данных осуществляет комиссия, созданная приказом Института.

6.5.4. Способы уничтожения персональных данных устанавливаются в локальных нормативных актах Института.

7. Требования к защите персональных данных при их обработке в информационных системах персональных данных

7.1. Требования к защите персональных данных при их обработке в информационных системах персональных данных определены постановлением

Правительства от 01.11.2012 №1119.

7.2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Закона о персональных данных. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

7.3. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор – Институт и филиалы, которые обрабатывают персональные данные (далее - оператор), или лицо (лица), осуществляющее обработку персональных данных – работники Отдела кадров, Бухгалтерии, Планово-экономического отдела Института и филиалов, по поручению оператора на основании заключаемого с этими лицами договора (далее - уполномоченные лица). Договор между оператором и уполномоченными лицами должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе.

7.4. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Закона о персональных данных.

7.5. Информационная система Института и филиалов «1С:Зарплата и кадры» или «Парус» является информационной системой, обрабатывающей персональные данные только своих сотрудников.

7.6. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

7.7. Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

7.8. Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

7.9. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе (например, угрозы, связанные с человеческим фактором).

7.10. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится Институтом и филиалами с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Закона о персональных данных, и в соответствии с нормативными правовыми актами, принятыми

во исполнение части 5 статьи 19 Закона о персональных данных.

7.11. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

7.12. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных (Институт не обрабатывает такие категории данных);

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории данных).

7.13. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные (Институт обрабатывает данную категорию данных);

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории данных);

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные (Институт не обрабатывает такие категории данных);

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории данных);

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории данных);

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории данных).

7.14. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории

данных);

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории данных);

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории данных);

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные (Институт не обрабатывает такие категории данных);

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории данных).

7.15. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные (Институт обрабатывает такие категории данных);

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора (Институт не обрабатывает такие категории данных).

7.16. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

7.17. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 16 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных

данных в информационной системе.

7.18. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 17 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

7.19. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных пунктом 18 настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

7.20. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

8. Заключительные положения

8.1. Настоящая Политика вступает в силу с момента ее утверждения директором Института и действует бессрочно, до замены ее новым.

8.2. Все изменения в Политику вносятся приказом Института.

Приложение № 3
к приказу от 23.10.2023 № 157 П

Федеральное государственное бюджетное учреждение науки
ИНСТИТУТ ОКЕАНОЛОГИИ им. П.П. ШИРШОВА
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ИО РАН)

УТВЕРЖДЕНО
приказом директора
от 23.10.2023 № 157 П

ПОЛОЖЕНИЕ
о внутреннем контроле и (или) аудите соответствия обработки персональных данных требованиям законодательства Российской Федерации

1. Общие положения

1.1. Настоящее Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в Федеральном государственном бюджетном учреждении науки Институте океанологии им. П.П. Ширшова Российской академии наук (далее – ИО РАН) требованиям законодательства в сфере обработки персональных данных (далее – Положение) разработано в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок осуществления внутреннего контроля и (или) аудита соответствия обработки персональных данных в ИО РАН и его филиалах требованиям к защите персональных данных, установленным законодательством Российской Федерации.

1.3. Исполнение Положения обязательно для всех работников ИО РАН и его филиалов, осуществляющих обработку персональных данных, как без использования средств автоматизации, так и в информационных системах обработки персональных данных.

1.4. В Положении используются основные понятия в значениях, определенных статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.5. **Внутренний контроль соответствия обработки персональных данных** – контроль соответствия обработки персональных данных в ИО РАН и его филиалов требованиям законодательства в сфере обработки персональных данных, проводимый силами ИО РАН и его филиалами в соответствии с Положением и другими локальными нормативными актами ИО РАН.

1.6. **Внутренний аудит соответствия обработки персональных данных** – контроль соответствия обработки персональных данных в ИО РАН и его филиалов требованиям законодательства в сфере обработки персональных данных, проводимый специализированными организациями, привлекаемыми ИО РАН по договорам оказания услуг в соответствии с Положением и другими локальными нормативными актами ИО РАН.

2. Формирование плана проведения внутреннего контроля

2.1. Проверки, осуществляемые в рамках внутреннего контроля, могут быть плановыми и внеплановыми.

2.2. Плановый контроль при обработке персональных данных проводится не реже 1 раза в год на основании плана, утвержденного приказом ИО РАН. Срок проведения планового внутреннего контроля составляет не более 10 рабочих дней.

2.3. Внеплановый контроль проводится на основании поступившего письменного или устного обращения от субъекта персональных данных о нарушении законодательства в области персональных данных. Внеплановый внутренний контроль должен быть завершен не позднее 30 дней со дня принятия решения о его проведении. О результатах внепланового внутреннего контроля информируется заинтересованное лицо.

2.4. План проведения внутренних проверок должен содержать следующую информацию:

– наименование мероприятия (внутренних проверок);
– периодичность мероприятий (внутренних проверок);
– планируемые даты мероприятий (внутренних проверок);
– перечень лиц, ответственных за проведение мероприятий (внутренних проверок).

2.5. Ежегодный план проведения внутренних проверок утверждается приказом ИО РАН.

3. Порядок проведения плановых (внеплановых) внутренних проверок режима обработки и защиты персональных данных

3.1. Внутренние проверки проводятся лицами, ответственными за проведение контрольных мероприятий согласно Плану проведения внутренних проверок, с привлечением при необходимости иных работников ИО РАН и его филиалов.

3.2. Внутренние проверки проводятся при непосредственном участии работников ИО РАН и его филиалов, осуществляющих обработку персональных данных.

3.3. Контроль соответствия условий обработки персональных данных осуществляется непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест работников ИО РАН и его филиалов, участвующих в процессе обработки персональных данных.

3.4. Внеплановые проверки соответствия обработки персональных данных установленным требованиям проводятся на основании поступившей информации о нарушении правил обработки персональных данных в ИО РАН и его филиалов. Проведение внеплановой проверки организуется Комиссией в течение трех рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.

3.5. При проведении внутреннего контроля должны быть установлены:

– порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
– соблюдение мер по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации;
– эффективность принимаемых мер по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных;
– состояние учета электронных носителей персональных данных;
– соблюдение правил доступа к персональным данным;
– порядок и условия применения средств защиты информации;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

– осуществление мероприятий по обеспечению целостности персональных данных;

– соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки персональных данных;

– наличие правовых оснований по сбору копий документов, содержащих персональные данные.

3.6. По результатам проведения внутренней проверки лицом, ответственным за проведение мероприятия согласно Плану проведения внутренних проверок, оформляется Акт о результатах проведения внутренней проверки режима обработки и защиты персональных данных в ИО РАН и его филиалов (далее - Акт о результатах проведения внутренней проверки). Форма Акта о результатах проведения внутренней проверки приведена в Приложении № 1 к настоящему Положению.

3.7. В случае выявления нарушений обработки персональных данных установленным требованиям сведения о выявленных нарушениях фиксируются в Акте о результатах проведения внутренней проверки.

3.8. Акт о результатах проведения внутренней проверки предоставляется Комиссии лицом, ответственным за проведение мероприятия согласно Плану проведения внутренних проверок.

3.9. Для устранения нарушений, выявленных по результатам внутренних проверок, Комиссия формирует План мероприятий по устранению нарушений, выявленных в результате проведения внутренней проверки режима обработки и защиты персональных данных в ИО РАН и его филиалов (далее - План мероприятий по устранению нарушений). Форма Плана мероприятий по устранению нарушений приведена в Приложении № 2 к настоящему Положению.

3.10. По результатам проведения мероприятий, включенных в ежегодный План проведения внутренних проверок Комиссия ежегодно или по запросу руководителя ИО РАН и его филиалов формирует отчет о выполнении плана проведения внутренних проверок режима обработки и защиты персональных данных в ИО РАН и его филиалов.

3.11. Отчет по результатам внутреннего контроля Комиссия направляет директору ИО РАН (руководителю филиала).

4. Порядок проведения внутреннего аудита

4.1. Внутренний аудит соответствия обработки персональных данных проводится в случаях, когда ИО РАН и его филиалы не могут объективно оценить соответствие обработки персональных данных в ИО РАН и его филиалах требованиям законодательства в сфере обработки персональных данных.

4.2. Внутренний аудит организуется на основании приказа ИО РАН.

4.3. Внутренний аудит проводит организация, которая в соответствии со своими учредительными документами занимается оценкой рисков в обработке персональных данных и возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

4.4. На время проведения внутреннего аудита директор ИО РАН (руководитель филиала) назначает ответственного работника, который должен взаимодействовать с организацией, проводящей аудит (далее – аудитор).

4.5. Ответственный работник обязан:

– обеспечить аудитора всей необходимой информацией;

– организовать условия для работы;

– оказывать помощь при возникновении трудностей;

– контролировать работу аудитора;

– принимать все отчеты аудитора и доводить их до сведения руководителя ИО РАН (филиала).

4.6. Действия и обязанности аудитора определяются заключенным договором оказания услуг по проведению внутреннего аудита.

5. Заключительные положения

5.1. Настоящее Положение вступает в силу с момента ее утверждения директором ИО РАН и действует бессрочно, до замены ее новым.

5.2. Все изменения в Положения вносятся приказом ИО РАН.

Приложение № 1
к Положению о внутреннем контроле и (или) аудите соответствия обработки персональных данных требованиям законодательства Российской Федерации

АКТ № _____
внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации

_____ от_____

Комиссия ИО РАН (филиала) в составе:

1. ….
2. ….
3. …

провела внутренний контроль соответствия обработки персональных данных в ИО РАН/филиале требованиям законодательства в сфере обработки персональных данных в соответствии с планом внутреннего контроля на _____ год, утвержденным приказом директора ИО РАН от _____ № _____.

В ходе проведения внутреннего контроля были выявлены следующие нарушения:

1. …
2. …
3. …

Подписи членов комиссии:

1. _____ _____
(ФИО, должность) (подпись)
2. _____ _____
(ФИО, должность) (подпись)
3. _____ _____
(ФИО, должность) (подпись)

Приложение № 2
к Положению о внутреннем контроле и (или) аудите соответствия обработки персональных данных требованиям законодательства Российской Федерации

ПЛАН
мероприятий по устранению нарушений, выявленных в результате проведения внутренней проверки режима обработки и защиты персональных данных в ИО РАН и его филиалов и их предупреждению в дальнейшей деятельности
(Акт внутренней проверки от __.__.____ № ___)

№ п/п	Выявленные нарушения в соответствии с актом проверки	Мероприятия по устранению выявленных нарушений и их предупреждению в дальнейшей деятельности	Срок исполнения	Ответственные исполнители	Примечание
1	2	3	4	5	6

Приложение № 4
к приказу от 23.10.2023 № 157 П

СОГЛАСИЕ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____,
(фамилия, имя, отчество)
паспорт серия _____ номер _____, кем и когда выдан _____
_____,
код подразделения _____, проживающий (ая) по адресу: _____
(индекс, полный адрес)
_____
_____,
в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие Федеральному государственному бюджетному учреждению науки **Институт океанологии им. П.П. Ширшова** Российской академии наук, расположенному по адресу: 117218, г. Москва, Нахимовский пр-т, д. 36, на автоматизированную, а также без использования средств автоматизации, обработку моих персональных данных, а именно совершение действий, предусмотренных п. 3 ч. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Политикой в отношении обработки персональных данных, утвержденной приказом ИО РАН от … № …, со сведениями о фактах, событиях и обстоятельствах моей жизни.

Цель обработки персональных данных:

- обеспечение соблюдения требований законодательства Российской Федерации;
- оформление и регулирование трудовых отношений;
- отражение информации в кадровых документах;
- начисление заработной платы;
- исчисление и уплата налоговых платежей, предусмотренных законодательством Российской Федерации;
- предоставление установленной отчетности в отношении физических лиц в ИФНС и внебюджетные фонды;
- подача сведений в банк для оформления банковской карты и последующего перечисления на нее заработной платы;
- предоставление налоговых вычетов;
- обеспечение безопасных условий труда;
- исполнение обязательств, предусмотренных научно-производственной деятельностью и договорами

_____
(указать какими)
_____
(указать иные цели, при наличии)

Перечень персональных данных, на обработку которых дается согласие:

Моими персональными данными является любая информация, относящаяся ко мне как субъекту персональных данных, указанная в трудовом договоре, личной карточке работника, трудовой книжке и полученная в течение срока действия моего трудового договора, в том числе: мои фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, реквизиты документа, удостоверяющего личность, идентификационный номер налогоплательщика, дата постановки его на учет, реквизиты постановки на учет в налоговом органе; номер страхового свидетельства государственного пенсионного страхования, дата регистрации в системе обязательного пенсионного страхования; адреса фактического места

проживания и регистрации по месту жительства и (или) по месту пребывания; почтовые и электронные адреса, номера телефонов, фотографии, сведения об образовании, профессии, специальности и квалификации, семейном положении и составе семьи; сведения об имущественном положении, доходах, задолженности; занимаемых ранее должностях и стаже работы, воинской обязанности, воинском учете; сведения о трудовом договоре и его исполнении (занимаемые должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной переподготовке, поощрениях и взысканиях, видах и периодах отпуска, временной нетрудоспособности, социальных льготах, командировании, рабочем времени и пр.), а также о других договорах (индивидуальной, коллективной материальной ответственности, ученических и т. п.), заключаемых при исполнении трудового договора.

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных: обработка вышеуказанных персональных данных будет осуществляться путем смешанной (автоматизированной, не автоматизированной) обработки персональных данных, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Обработка вышеуказанных персональных данных будет осуществляться путем _____ обработки персональных данных.

(указать способ обработки (смешанной, автоматизированной, неавтоматизированной)

Даю согласие на передачу (предоставление) оператором моих данных: _____

_____*(ОГРН: _____ ИНН: _____)*

(указать полное наименование юридического лица, фамилия, имя, отчество и адрес физического лица передачу которым дается согласие)

путем

_____

(предоставления, допуска)

Настоящее согласие действует в течение срока действия моего трудового договора с целью осуществления трудовых отношений и до даты окончания трудового договора (трудовых отношений) и может быть отозвано мной в любое время путем подачи оператору заявления в простой письменной форме.

Персональные данные субъекта подлежат хранению в течение сроков, установленных законодательством Российской Федерации.

Персональные данные уничтожаются по достижению целей обработки персональных данных; при ликвидации или реорганизации оператора; на основании письменного обращения субъекта персональных данных с требованием о прекращении обработки его персональных данных (оператор прекратит обработку таких персональных данных в течение 3 (трех) рабочих дней, о чем будет направлено письменное уведомление субъекту персональных данных в течение 10 (десяти) рабочих дней.

« ____ » _____ 20 ____ г. _____

(дата) (подпись)

Приложение № 5
к приказу от 23.10.2023 № 157 П

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации (персональных данных), не содержащих сведений, составляющих государственную тайну.

Я,_____ паспорт _____
(ФИО сотрудника, номер паспорта)
выдан _____
(кем и когда выдан)
Проживающий по адресу: _____
(адрес регистрации и фактического проживания)
исполняющий(ая) должностные обязанности по занимаемой должности:

_____
(должность, наименование структурного подразделения)

предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностной инструкцией (регламентом), мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащим сведений, составляющих государственную тайну. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.

4. Не использовать конфиденциальные сведения с целью получения выгоды.

5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.

6. В течение 3-х лет после прекращения права на допуск к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

– Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации, а именно:

– за нарушение неприкосновенности частной жизни (статья 137 УК РФ);

– за причинение лицу убытков в результате нарушения правил обработки его персональных данных (возмещение убытков);

– за причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных (статья 24 Закона о персональных данных, ст. 151 ГК РФ).

_____ _____
(фамилия, инициалы) *(подпись)*

«_____»_____202__г.