Приложение № 2
к приказу от 23.08.2022 г. № 2/ПД

ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В БЛАГОТВОРИТЕЛЬНОМ ФОНДЕ «ПОДСОЛНУХ»

Москва, 2022 г.

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Положение об организации обеспечения безопасности персональных данных при их обработке в БЛАГОТВОРИТЕЛЬНОМ ФОНДЕ «ПОДСОЛНУХ» (далее – Положение) разработано в соответствии с статьями 18.1, 19 Федерального закона от 27.07.2006 № 152–ФЗ «О персональных данных» (далее – ФЗ–152) и определяет порядок обработки персональных данных, а также устанавливает требования к обеспечению безопасности персональных данных, обрабатываемых в БЛАГОТВОРИТЕЛЬНОМ ФОНДЕ «ПОДСОЛНУХ» (далее – Оператор).

Действия настоящего Положения распространяются на обработку персональных данных как с использованием средств автоматизации, так и без использования таких средств.

Нормы и правила, содержащиеся в настоящем Положении, являются обязательными для исполнения всеми работниками Оператора, исполнителями по гражданско-правовым договорам при выполнении работ (оказании услуг).

2. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Назначение ответственных лиц

Для организации обработки и обеспечения безопасности ПДн у Оператора назначаются ответственные лица.

В своей работе ответственный за организацию обработки ПДн руководствуется инструкцией ответственного за организацию обработки персональных данных.

В своей работе ответственный за обеспечение безопасности ПДн в информационных системах руководствуется инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах.

2.2 Допуск к персональным данным

Работники Оператора допускаются к обработке ПДн в объеме, необходимом им для выполнения должностных обязанностей.

Перед началом работы с ПДн работники Оператора, допущенные к ПДн, обязаны:

– ознакомиться под роспись с положениями законодательства Российской Федерации о персональных данных;

– ознакомиться под роспись с настоящим Положением;

– пройти инструктаж и обучение по работе с ПДн;

– пройти инструктаж и обучение по работе с ПДн в информационных системах ПДн.

Форма соглашения о неразглашении информации, содержащей персональные данные при их обработке Оператором, представлена в Приложении № 1 к настоящему Положению.

В случае если на основании договоров, заключенных с юридическими или физическими лицами, Оператору необходимо предоставить таким лицам доступ к ПДн, то соответствующие ПДн предоставляются Оператором только после подписания Соглашения об обеспечении безопасности персональных данных, порученных на обработку соглашения, или включения в договоры положений о конфиденциальности при обработке ПДн.

Государственным органам, осуществляющим функции контроля (надзора), права доступа к ПДн предоставляются только в сфере их компетенции и в объеме, предусмотренном действующим законодательством.

Методы и правила разграничения доступа определяются, исходя из целесообразности и эффективности их применения. Технические средства должны обладать возможностью реализации выбранного метода разграничения доступа.

2.3 Получение персональных данных

ПДн следует получать лично у субъекта ПДн или от его законного представителя. В случае если ПДн возможно получить только у третьей стороны, Оператор до начала обработки таких ПДн обязан уведомить субъект ПДн о получении его ПДн. Помимо адреса и наименования организации Оператор должен сообщить субъекту ПДн о целях обработки ПДн, источниках получения и предполагаемых пользователях ПДн, а также сведения о его правах, установленных ФЗ-152.

Оператор освобождается от обязанности предоставить субъекту персональных данных указанные выше сведения, если:

- субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим Оператором;
- ПДн получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника персональных данных (в том числе справочники, адресные книги);
- Оператор осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;
- предоставление субъекту ПДн указанных выше сведений нарушает права и законные интересы третьих лиц.

2.4 Передача персональных данных

Передача ПДн субъектов ПДн третьим лицам может осуществляться только при наличии согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, в целях исполнения условий договора, а также в случаях, установленных законодательством Российской Федерации.

Передача ПДн субъектов должна осуществляться только между работниками Оператора, допущенными к обработке ПДн.

2.5 Хранение персональных данных

Хранение ПДн субъектов осуществляется на бумажных и машинных носителях информации в специально выделенных хранилищах Оператора, а также в ИСПДн Оператора, обеспечивающих сохранность ПДн и их защиту от несанкционированного доступа.

Уничтожение ПДн в ИСПДн, на машинных и бумажных носителях информации должно производиться в течение 30 (тридцати) дней с даты достижения цели обработки (предельного срока хранения) ПДн. При невозможности уничтожения ПДн в течение тридцати дней с даты достижения цели обработки ПДн, обеспечивается их блокирование и уничтожение в срок, не превышающий 6 (шести) месяцев.

2.6 Уведомление об обработке персональных данных

Согласно ст. 22 ФЗ–152 Оператор уведомляет уполномоченный орган по защите прав субъектов ПДн об обработке ПДн.

В случае изменения сведений, указанных в уведомлении, а также в случае прекращения обработки ПДн Оператор также уведомляет об этом Уполномоченный орган в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн.

3. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

Работники Оператора, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки.

ПДн при их обработке без использования средств автоматизации обособляются от иной информации путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается запись на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы. При обработке различных категорий ПДн без использования средств автоматизации для каждой категории ПДн должен использоваться отдельный материальный носитель.

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

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, 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 должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, при необходимости получения письменного согласия на обработку ПДн;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

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

Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

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

Уточнение ПДн при их обработке без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна производиться таким образом, чтобы можно было определить места хранения персональных данных (материальных носителей).

4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Организация защиты персональных данных

Оператор при обработке ПДн обязан принимать необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Для обеспечения безопасности ПДн применяются следующие меры:

- определение угроз безопасности ПДн при их обработке в ИСПДн;
- применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- ведение учета машинных носителей ПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

- контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

ПДн обрабатываются у Оператора как с использованием средств автоматизации, так и без использования таких средств.

Защита ПДн от неправомерного их использования или утраты обеспечивается Оператором за счет собственных средств.

В отсутствие работника на его рабочем месте не должно быть документов и машинных носителей информации, содержащих ПДн.

Доступ работников Оператора в помещения, в которых осуществляется обработка и хранение ПДн, ограничивается организационными мерами.

Организацию обработки ПДн субъектов и контроль соблюдения мер их защиты работниками, которых имеют доступ к ПДн, осуществляют руководители проектов.

Организация защиты ПДн, обрабатываемых в ИСПДн, осуществляется в рамках действующей системы защиты.

Разработка и осуществление мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, может осуществляться сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.

4.2 Обеспечение безопасности персональных данных при взаимодействии Оператора с третьими лицами

В целях обеспечения безопасности ПДн при взаимоотношении Оператора с третьими лицами должны выполняться следующие меры:

- должно быть подписано Соглашение об обеспечении безопасности персональных данных, порученных на обработку, или включения в договоры положений о конфиденциальности при обработке ПДн.;
- должен проводиться мониторинг действий третьих лиц в ИСПДн Оператора.

В случае заключения с юридическим лицом договора, одним из условий которого является передача юридическому лицу персональных данных, обрабатываемых Оператором на законных основаниях, Оператор должен удостовериться до заключения договора в адекватном уровне обеспечения юридическим лицом безопасности ПДн. Обязательным является наличие доказательств выполнения действующего законодательства Российской Федерации в области обеспечения безопасности ПДн.

Любое соединение с внешней информационной системой должно быть согласовано с ответственным за организацию обработки ПДн и ответственным за обеспечение безопасности ПДн в информационных системах. Любой доступ должен быть ограничен и протестирован на возможные уязвимости. Внешний доступ должен также отвечать следующим характеристикам:

- необходимо подписание владельцем внешней информационной системы соглашения о принятии на себя обязательств по обеспечению безопасности ПДн в своей части сети, соединенной с сетью Оператора;
- должен быть обеспечен контроль доступа и аутентификация.

5. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Лица, нарушающие или не исполняющие требования настоящего Положения, могут быть привлечены к дисциплинарной, административной или уголовной ответственности в порядке, предусмотренном действующим законодательством РФ,

5.2. Руководители проектов Оператора несут персональную ответственность за исполнение обязанностей их подчиненными.

6. ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Внесение изменений в настоящее Положение осуществляется в следующих случаях:
- при внесении новых требований к обработке и обеспечению безопасности ПДн со стороны российского законодательства и государственных органов, осуществляющих функции контроля (надзора);
- по результатам проверок государственных органов, осуществляющих функции контроля (надзора), выявивших несоответствия требованиям по обработке и обеспечению безопасности ПДн;
- по результатам внутреннего контроля (аудита) системы защиты ПДн в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн и выявивших недостатки в правилах предоставления доступа к ПДн.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Повседневный контроль порядка обращения с ПДн осуществляют руководители проектов, в рамках реализации которых обрабатываются ПДн.

Периодический контроль выполнения настоящего Положения возлагается на ответственного за организацию обработки ПДн и ответственного за обеспечение безопасности ПДн в информационных системах.

ПРИЛОЖЕНИЕ № 1

Лист ознакомления работника с порядком обработки персональных данных в БЛАГОТВОРИТЕЛЬНОМ ФОНДЕ «ПОДСОЛНУХ»

Я, _____,
(Фамилия, имя, отчество)

выполняющий(ая) должностные обязанности по занимаемой должности _____ *(должность)* в БЛАГОТВОРИТЕЛЬНОМ ФОНДЕ «ПОДСОЛНУХ» (далее – Оператор), в период трудовых отношений и в течение пяти лет с даты их прекращения обязуюсь не разглашать и не передавать третьим лицам и неуполномоченным на это работникам Оператора персональные данные, обрабатываемые Оператором, которые мне доверены (будут доверены) или станут известны в связи с выполнением моих должностных обязанностей.

Я подтверждаю, что ознакомлен с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными нормативными актами по вопросам обеспечения безопасности персональных данных при их обработке, в том числе:

- Приложение № 2 к Приказу от 23.08.2022 № 2/ПД «Положение об организации обеспечения безопасности персональных данных при их обработке в БЛАГОТВОРИТЕЛЬНОМ ФОНДЕ «ПОДСОЛНУХ»;
- Инструкция работника, допущенного к обработке персональных данных.

Я также подтверждаю, что в ходе работы получаю доступ к следующим категориям персональных данных, обрабатываемых без использования средств автоматизации:

- персональные данные, не являющиеся специальными или биометрическими;
- персональные данные, являющиеся специальными;
- персональные данные, являющиеся биометрическими.

Я предупрежден(а), что в случае нарушения порядка работы с персональными данными буду привлечен(а) к ответственности в соответствии с действующим законодательством Российской Федерации.

_____	_____	_____
(должность)	(подпись)	(ФИО)

«____»_____ 20 _____ г.

Лист ознакомления лица, привлеченного по договору гражданско-правового характера, с порядком обработки персональных данных в БЛАГОТВОРИТЕЛЬНОМ ФОНДЕ «ПОДСОЛНУХ»

Я, _____,
(Фамилия, имя, отчество)

как лицо, привлеченное по договору гражданско-правового характера, заключенному с БЛАГОТВОРИТЕЛЬНЫМ ФОНДОМ «ПОДСОЛНУХ» (далее – Оператор), в период гражданско-правовых отношений и в течение пяти лет с даты их прекращения, обязуюсь не разглашать персональные данные, обрабатываемые Оператором, которые будут мне доверены или станут мне известны в ходе исполнения мною своих обязанностей.

Я также подтверждаю, что ознакомлен с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки и обеспечения безопасности персональных данных, в том числе:

- Приложение № 2 к Приказу от 23.08.2022 № 2/ПД «Положение по организации обработки обеспечения безопасности персональных данных при их обработке в БЛАГОТВОРИТЕЛЬНОМ ФОНДЕ «ПОДСОЛНУХ»;
- Инструкция работника, допущенного к обработке персональных данных.

Я также подтверждаю, что в ходе оказания услуг (выполнения работ) получаю доступ к следующим категориям персональных данных, обрабатываемых без использования средств автоматизации:

- персональные данные, не являющиеся специальными или биометрическими;
- персональные данные, являющиеся специальными;
- персональные данные, являющиеся биометрическими.

Я предупрежден(а), что в случае нарушения порядка работы с персональными данными буду привлечен(а) к ответственности в соответствии с действующим законодательством Российской Федерации.

_____	_____	_____
(должность)	(подпись)	(ФИО)

«____»_____ 20 _____ г.

ПРИКАЗ

23 августа 2022 г. № 2/ПД

г. Москва

Об утверждении локальных актов
по персональным данным
Благотворительного Фонда «ПОДСОЛНУХ»

В целях актуализации локальных актов по персональным данным и повышения эффективности организации работы по обработке и защите персональных данных в Благотворительном Фонде «ПОДСОЛНУХ», руководствуясь Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Политику в отношении обработки персональных данных Благотворительного Фонда «ПОДСОЛНУХ» (Приложение № 1) в новой редакции с 23.08.2022 г.
2. Утвердить и ввести в действие Положение об организации обеспечения безопасности персональных данных при их обработке в Благотворительном Фонде «ПОДСОЛНУХ» (Приложение № 2) в новой редакции с 23.08.2022 г.
3. Считать утратившей силу Политику БФ «ПОДСОЛНУХ» в отношении обработки персональных данных, утвержденную приказом от 29.10.2020 г. № 29-10/2020 «О назначении лиц, ответственных за обработку и защиту персональных данных, и утверждении документов по персональным данным» с 23.08.2022 г.
4. Считать утратившим силу Положение по организации обработки и обеспечению безопасности персональных данных в БФ «ПОДСОЛНУХ», утвержденное приказом от 29.10.2020 г. № 29-10/2020 «О назначении лиц, ответственных за обработку и защиту персональных данных, и утверждении документов по персональным данным» с 23.08.2022 г.
5. Ответственному за организацию обработки персональных данных Посадковой М.В. обеспечить ознакомление работников Благотворительного Фонда «ПОДСОЛНУХ» с

локальными нормативными актами по персональным данным, указанными в пунктах 1,2 настоящего приказа в срок до 15.12.2022 г.

6. Ответственному за организацию обработки персональных данных Посадковой М.В. осуществлять контроль за размещением локальных нормативных актов в области персональных данных, указанных в пунктах 1,2 настоящего приказа, на официальном сайте Благотворительного Фонда «ПОДСОЛНУХ», на информационном портале propid.ru, назначенными лицами согласно Приложению № 3 к настоящему приказу.

7. Контроль за исполнением настоящего приказа оставляю за собой.

Президент И.В. Бакрадзе

С приказом ознакомлена М.В. Посадкова