НАЦИОНАЛЬНЫЙ РАСЧЕТНЫЙ ДЕПОЗИТАРИЙ
ГРУППА МОСКОВСКАЯ БИРЖА

Приложение
к приказу НКО АО НРД
от «17» 09. 2020 г. № 180

Политика обработки персональных данных в НКО АО НРД

ИБ.8-2020

Информация о документе

Владелец документа		Управление информационной безопасности	
Версия		1.0	
Дата		19.08.2020	
Версионность			
Версия	Дата	Автор	Описание
1.0.	19.08.2020	Заргаров Д.Е.	Разработка документа на основании требований закона от 27.07.2006 № 152-ФЗ «О персональных данных»

Оглавление

1. Область действия

1.1. Настоящий документ является документом первого уровня в структуре внутренних документов НРД по обеспечению ИБ, развивает положения «Политики информационной безопасности» НКО АО НРД и определяет частную политику по обеспечению ИБ при осуществлении обработки персональных данных.
1.2. Настоящая Политика обработки персональных данных в НКО АО НРД (далее – Политика) определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных в НКО АО НРД (далее – НРД) с целью защиты прав субъектов при обработке их персональных данных.
1.3. Политика обязательна для ознакомления и исполнения всеми лицами, допущенными к обработке персональных данных.

2. Общие положения

2.1. Настоящая Политика является общедоступным документом НРД и предусматривает возможность ознакомления с ней любых лиц.
2.2. В Политике используются термины и определения в соответствии с их значениями, как они определены в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
2.3. Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих вопросы обработки персональных данных работников, клиентов, контрагентов НРД.
2.4. Политика распространяется на всех работников, клиентов, контрагентов НРД. Требования Политики также учитываются и предъявляются в отношении иных лиц при необходимости их участия в процессе обработки персональных данных НРД, а также в случаях передачи им в установленном порядке персональных данных на основании соглашений, договоров, поручений на обработку.
2.5. Политика действует бессрочно с момента утверждения до утверждения новой редакции Политики или отмены.

3. Термины, определения, сокращения

3.1. Термины, определения и сокращения, используемые в настоящем документе на основании Политики информационной безопасности:
3.1.1. Автоматизированная обработка персональных данных - Обработка персональных данных с помощью средств вычислительной техники.
3.1.2. Блокирование персональных данных - Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
3.1.3. Информационная система персональных данных - Совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических средств.
3.1.3. Обезличивание персональных данных - Действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных.
3.1.4. Обработка персональных данных - Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
3.1.5. 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.
3.1.6. Персональные данные - Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
3.1.7. Предоставление персональных данных - Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
3.1.8. Трансграничная передача персональных данных - Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу.
3.1.9. Распространение персональных данных - Действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

Используемые сокращения:
152-ФЗ – Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»
ИСПДн – Информационная система персональных данных
НРД – НКО АО НРД
ПД – Персональные данные
ФЗ – Федеральный закон

4. Принципы и условия, особенности обработки персональных данных

4.1. Принципы обработки. Обработка персональных данных в НРД осуществляется на основе следующих принципов:
4.1.1. законности и справедливой основы;
4.1.2. ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;
4.1.3. недопущения обработки ПД, несовместимой с целями сбора персональных данных;
4.1.4. недопущения объединения баз данных, содержащих ПД, обработка которых осуществляется в целях, несовместимых между собой;
4.1.5. обработки только тех ПД, которые отвечают целям их обработки;
4.1.6. соответствия содержания и объема обрабатываемых ПД заявленным целям обработки;
4.1.7. недопущения обработки ПД, избыточных по отношению к заявленным целям их обработки;
4.1.8. обеспечения точности, достаточности и актуальности ПД по отношению к целям их обработки;
4.1.9. уничтожения либо обезличивания ПД по достижении целей их обработки, в случае утраты необходимости в достижении этих целей или при невозможности устранения НРД допущенных нарушений при обработке ПД, если иное не предусмотрено федеральным законом.

4.2. Условия обработки. НРД обрабатывает персональные данные в следующих случаях:
4.2.1. получено согласие субъекта персональных данных (далее – субъекта) на обработку его ПД,
4.2.2. обработка ПД необходима для:
- достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на НРД функций, полномочий и обязанностей;
- осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект, а также для заключения договора по инициативе субъекта или договора, по которому субъект будет являться выгодоприобретателем или поручителем;
- осуществления прав и законных интересов НРД или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта,

4.2.3. доступ к ПД предоставлен субъектом ПД либо по его просьбе неограниченному кругу лиц (далее – общедоступные персональные данные),
4.2.4. данные подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.3. Конфиденциальность
4.3.1. НРД и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта, если иное не предусмотрено федеральным законом.

4.4. Общедоступные источники
4.4.1. В целях информационного обеспечения в НРД могут создаваться общедоступные источники ПД, в том числе справочники и адресные книги. В общедоступные источники с письменного согласия субъекта (согласия, полученного в письменной форме) могут включаться сообщаемые субъектом его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адрес электронной почты, фотография и иные персональные данные.

4.4.2. Сведения о субъекте должны быть в любое время исключены из общедоступных источников персональных данных по его требованию либо по решению суда или иных уполномоченных государственных органов.

4.5. Специальные категории ПД

4.5.1. Обработка специальных категорий ПД, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни в НРД не производится.

4.5.2. Обработка НРД специальных категорий ПД, касающихся состояния здоровья допускается только в отношении сотрудников НРД и в случаях, если:

4.5.2.1. субъект дал согласие в письменной форме на обработку своих ПД;

4.5.2.2. ПД сделаны субъектом общедоступными;

4.5.2.3. обработка ПД осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

4.5.2.4. обработка ПД необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта невозможно;

4.5.2.5. обработка ПД необходима для установления или осуществления прав субъекта или третьих лиц, а равно и в связи с осуществлением правосудия;

4.5.2.6. обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

4.5.3. Обработка специальных категорий ПД незамедлительно прекращается, если устранены причины, вследствие которых осуществлялась их обработка, если иное не установлено федеральным законом.

4.5.4. Обработка ПД о судимости может осуществляться НРД исключительно в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4.6. Биометрические ПД

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления личности субъекта, в НРД не обрабатываются.

4.7. Поручение обработки другому лицу

4.7.1. НРД вправе поручить обработку ПД другому лицу с согласия субъекта, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее - поручение оператора). Лицо, осуществляющее обработку ПД по поручению НРД, обязано соблюдать принципы и правила обработки ПД, предусмотренные 152-ФЗ.

4.7.2. Лицо, осуществляющее обработку ПД по поручению НРД, не обязано получать согласие субъекта на обработку его ПД.

4.7.3. В случае, если НРД поручает обработку ПД другому лицу, ответственность перед субъектом за действия указанного лица несет НРД. Лицо, осуществляющее обработку ПД по поручению НРД, несет ответственность перед НРД.

4.8. Трансграничная передача

4.8.1. НРД до начала осуществления трансграничной передачи ПД убеждается в том, что иностранным государством, на территорию которого предполагается осуществлять передачу ПД, обеспечивается адекватная защита прав субъектов.

4.8.2. Трансграничная передача ПД на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов, может осуществляться в случаях:

4.8.2.1. наличия письменного согласия субъекта на трансграничную передачу его ПД;

4.8.2.2. исполнения договора, стороной которого является субъект;

4.8.2.3. защиты жизни, здоровья, иных жизненно важных интересов субъекта или других лиц при невозможности получения письменного согласия субъекта.

5. Обеспечение безопасности персональных данных

5.1. Безопасность ПД, обрабатываемых НРД, обеспечивается реализацией правовых, организационных и технических мер, необходимых для обеспечения требований федерального законодательства в области защиты ПД.

5.2. Для предотвращения несанкционированного доступа к ПД НРД применяются следующие организационно-технические меры:

5.2.1. назначение должностных лиц, ответственных за организацию обработки и за обеспечение безопасности ПД;
5.2.2. ограничение и разграничение доступа сотрудников и иных лиц к ПД и средствам обработки, мониторинг действий с ПД;
5.2.3. ознакомление субъектов с требованиями федерального законодательства и внутренних нормативных документов НРД по обработке и защите ПД;
5.2.4. организация учета, хранения и обращения носителей информации, содержащих ПД;
5.2.5. проверка наличия в договорах и включение при необходимости в договоры пунктов об обеспечении конфиденциальности ПД;
5.2.6. определение угроз безопасности ПД при их обработке, формирование на их основе модели угроз;
5.2.7. проверка готовности и эффективности использования средств защиты информации;
5.2.8. регистрация и учет действий пользователей ИСПДн;
5.2.9. применение средств обеспечения безопасности (антивирусных средств, межсетевых экранов, средств защиты от несанкционированного доступа, средств криптографической защиты информации), в том числе прошедших процедуру оценки соответствия в установленном порядке;
5.2.10. организация пропускного режима на территорию НРД, охраны помещений с техническими средствами обработки ПД;
5.2.11. осуществление внутреннего контроля за соблюдением установленного порядка, проверка эффективности принятых мер, реагирование на инциденты.

6. Права субъекта персональных данных

6.1. Согласие субъекта на обработку его персональных данных
6.1.1. Субъект принимает решение о предоставлении его ПД и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПД может быть дано субъектом персональных данных или его законным представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.
6.1.2. Обязанность предоставить доказательство получения согласия субъекта на обработку его ПД или доказательство наличия оснований, указанных в ФЗ-152, возлагается на НРД.
6.1.3. Субъект имеет право отозвать согласие на обработку ПД, направив соответствующий запрос НРД по почте или обратившись лично, в том числе через своего законного представителя.

6.2. Права субъекта
6.2.1. Субъект имеет право на получение у НРД информации, касающейся обработки его ПД, если такое право не ограничено в соответствии с федеральными законами. Субъект вправе требовать от НРД уточнения, блокирования или уничтожения его ПД в случае, если ПД являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
6.2.2. Субъект имеет право дать предварительное согласие на обработку ПД с целью продвижения НРД своих товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи. Указанная обработка признается осуществляемой без предварительного согласия субъекта, если НРД не докажет, что такое согласие было получено.
6.2.3. НРД по требованию субъекта немедленно прекращает обработку его ПД в целях, указанных в пункте 6.2.2. настоящей Политики.
6.2.4. НРД на основании исключительно автоматизированной обработки ПД не принимает решений, порождающих юридические последствия в отношении субъекта или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных федеральными законами, или при наличии письменного согласия субъекта.
6.2.5. Если субъект считает, что НРД осуществляет обработку его ПД с нарушением требований ФЗ-152 или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие НРД путем подачи жалобы в уполномоченный орган по защите прав субъектов ПД или в судебном порядке.
6.2.6. Субъект имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7. Ответственность

7.1. Права и обязанности НРД определяются действующим законодательством, договорами и внутренними документами НРД.
7.2. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки ПД и руководителями подразделений, осуществляющих обработку ПД в пределах их полномочий.

7.3. Ответственность лиц, участвующих в обработке ПД на основании поручений НРД, за неправомерное использование персональных данных устанавливается в соответствии с условиями заключенного между НРД и контрагентом гражданско-правового договора или Соглашения о конфиденциальности информации.
7.4. Лица, виновные в нарушении положений, регулирующих обработку и защиту ПД, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами, локальными актами, договорами НРД.

8. Актуализация документа

8.1. Настоящая Политика пересматривается Управлением ИБ не реже 1 раза в год, а также при изменении законодательных и нормативных актов в области ПД, в случаях изменения перечня обрабатываемых ПД, ИСПДн, по результатам внутренних и внешних аудитов, изменениях в методиках и порядке осуществления работ, а также по инициативе руководителя НРД или руководителя УИБ, обоснованной инициативе иных заинтересованных сторон.

9. Нормативные правовые акты, в соответствии с которыми определяется Политика

Политика определяется в соответствии со следующими нормативными правовыми актами:
[1] Трудовой кодекс Российской Федерации;
[2] Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
[3] Постановление Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012;
[4] Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
[5] Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
[6] Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
[7] Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
[8] Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
[9] Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»;
[10] Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»;
[11] иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.