РОССИЯ, 117292, Г.МОСКВА, УЛ. ИВАНА БАБУШКИНА, Д.16А
8 (495) 785-70-75
WWW.METALLURGBANK.RU
MAIL@METALLURGBANK.RU

УТВЕРЖДЕНО

Председателем Правления
ООО РНКО «Металлург»
от «01» апреля 2022 года
(Приказ № 50)

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО РНКО «МЕТАЛЛУРГ»

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ ДОКУМЕНТА

1.1. Положение ООО РНКО «Металлург» (далее – РНКО) об обработке и защите персональных данных (далее – Положение) определяет позицию и намерения РНКО в области обработки и реализации требований к защите персональных данных лиц, состоящих в договорных, гражданско-правовых и иных отношениях с РНКО, соблюдения действующего законодательства Российской Федерации в области информационной безопасности, а также требований Федерального закона от 27.06.2006 года №152-ФЗ «О персональных данных», основной целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Положение предназначено для изучения и неукоснительного исполнения всеми сотрудниками РНКО, а также подлежит доведению до сведения лиц, состоящих в договорных, гражданско-правовых и иных отношениях с РНКО (далее – граждане), партнеров и других заинтересованных сторон.

1.3. Актуализация настоящего Положения осуществляется не реже 1 раза в год, или при изменении нормативных требований.

2 ОПРЕДЕЛЕНИЯ

2.1. Под персональными данными (далее – ПДн) понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (гражданину).

2.2. Под обработкой ПДн понимается любое действие (операция) или совокупность действий (операций) с ПДн, совершаемых с использованием средств автоматизации или без использования таких средств. К таким действиям (операциям) можно отнести: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

3 ОСНОВНЫЕ ПОЛОЖЕНИЯ

3.1. Понимая важность и ценность информации о человеке, РНКО обеспечивает надежную защиту предоставленных ПДн. РНКО обрабатывает ПДн только тех лиц, которые состоят в договорных, гражданско-правовых и иных отношениях с РНКО, а именно:

- лиц, состоящих в трудовых отношениях с РНКО (сотрудники РНКО);
- лиц, являющихся соискателями должностей в РНКО;
- лиц, являющихся Клиентами или Партнерами РНКО.

3.2. Под безопасностью ПДн РНКО понимает защищенность ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн и принимает необходимые правовые, организационные и технические меры для защиты ПДн.

3.3. Обработка ПДн сотрудников РНКО осуществляется в строгом соответствии с трудовым законодательством РФ. Данные клиентов РНКО, полученные в связи с заключением договора, стороной которого является субъект ПДн, обрабатываются с соблюдением принципов и условий обработки ПДн, установленных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон «О персональных данных»). РНКО не осуществляет распространение или раскрытие ПДн без согласия гражданина, если иное не предусмотрено федеральным законом.

3.4. Правовым основанием обработки ПДн является осуществление возложенных на РНКО законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, Федеральными законами, в частности: «О банках и банковской деятельности» № 395-1 от 02.12.1990 г., «О Центральном банке Российской Федерации (Банке России)» № 86-ФЗ от 10.07.2002 г., «О национальной платежной системе» № 161-ФЗ от 27.06.2011 г., «О кредитных историях» № 218-ФЗ от 30.12.2004 г., «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» № 115-ФЗ от 07.08.2001 г., «О валютном регулировании и валютном контроле» № 173-ФЗ от 10.12.2003 г., «О рынке ценных бумаг» № 39-ФЗ от 22.04.1996 г., «О страховании вкладов физических лиц в банках Российской Федерации» № 177-ФЗ от 23.12.2003 г., «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» № 27-ФЗ от 01.04.1996 г., «О персональных данных» № 152-ФЗ от 27.07.2006 г., «Об акционерных обществах» № 208-ФЗ от 26.12.1995, «Об электронной подписи» № 63-ФЗ от 06.04.2011 г., принятыми в их исполнение нормативными актами Банка России, а также в целях организации учета служащих кредитной организации для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия служащему в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также нормативными актами Банка России.

3.5. При обработке ПДн РНКО придерживается следующих принципов:

- РНКО осуществляет обработку ПДн только на законной и справедливой основе;
- обработка ПДн в РНКО ограничивается достижением конкретных, заранее определенных и законных целей;
- в РНКО не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

- до начала сбора/получения ПДн, РНКО определяет конкретные законные цели обработки ПДн;
- РНКО собирает только те ПДн, которые являются необходимыми и достаточными для заявленной цели обработки;
- РНКО систематически принимает меры по удалению или уточнению неполных или неточных данных;
- РНКО уничтожает либо обезличивает ПДн по достижении целей обработки или в случае утраты необходимости в достижении целей[1];
- РНКО не раскрывает третьим лицам и не распространяет персональные данные без согласия гражданина (если иное не предусмотрено действующим законодательством Российской Федерации);
- РНКО не осуществляет сбор и обработку персональных данных граждан, касающихся расовой, национальной принадлежности, политических, религиозных, философских и иных убеждений, состояния здоровья, интимной жизни, членства в общественных объединениях, в том числе в профессиональных союзах.

3.6. РНКО вправе поручить обработку персональных данных (с согласия гражданина[2]) юридическому лицу, на основании заключаемого с этим лицом договора, в котором указанные лица обязуются соблюдать принципы и правила обработки персональных данных, предусмотренные Законом «О персональных данных». В договоре (поручении Банка) должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность ПДн при их обработке.

3.7. В случае осуществления Банком трансграничной передачи ПДн граждан на территорию иностранного государства, указанная трансграничная передача должна осуществляться с соблюдением требований действующего законодательства Российской Федерации, а также международно-правовых актов. При этом получающей стороной могут быть страны, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн, а также иные иностранные государства при условии обеспечения адекватных защитных мер прав субъектов ПДн.

4 ПРАВА ГРАЖДАН В ЧАСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Гражданин, ПДн которого обрабатываются в РНКО имеет право:

- требовать от РНКО уточнения его ПДн их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отозвать свое согласие на обработку ПДн;
- требовать устранения неправомерных действий РНКО в отношении его ПДн;
- обжаловать действия или бездействие РНКО в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) или в судебном порядке в случае, если гражданин считает, что РНКО осуществляет обработку его ПДн с нарушением требований Закона «О персональных данных» или иным образом нарушает его права и свободы;

---

[1] Если иное не предусмотрено соглашением между РНКО и гражданином либо если РНКО не вправе осуществлять обработку ПДн без согласия гражданина на основаниях, предусмотренных Законом «О персональных данных» или другими федеральными законами.

[2] Если иное не предусмотрено федеральным законом.

- обжаловать действия или бездействие РНКО в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) или в судебном порядке в случае, если гражданин считает, что РНКО осуществляет обработку его ПДн с нарушением требований Закона «О персональных данных» или иным образом нарушает его права и свободы;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

4.2. Гражданин имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн РНКО;
- правовые основания и цели обработки ПДн;
- сведения о применяемых РНКО способах обработки ПДн;
- наименование и место нахождения РНКО;
- сведения о лицах (за исключением работников РНКО), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с РНКО или на основании федерального закона;
- перечень обрабатываемых ПДн, относящихся к гражданину, от которого поступил запрос и источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления гражданином прав, предусмотренных Законом «О персональных данных»;
- информацию об осуществляемой или о предполагаемой трансграничной передаче ПДн;
- наименование (Ф.И.О.) и адрес лица, осуществляющего обработку ПДн по поручению РНКО;
- иные сведения, предусмотренные Законом «О персональных данных» или другими федеральными законами.

5 ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ПОЛОЖЕНИЕ

5.1. Настоящее Положение подлежит изменению по мере необходимости, а также:

- при изменении законодательства Российской Федерации в области ПДн;
- при изменении состава лиц, которым РНКО поручает обработку ПДн;
- в случаях выявления несоответствий, затрагивающих обработку ПДн;
- по результатам контроля выполнения требований по обработке и защите ПДн;
- по решению руководства РНКО.

5.2. Актуальная версия настоящего Положения публикуется на официальном сайте РНКО – www.metallurgbank.ru.

6 ОТВЕТСТВЕННОСТЬ

6.1. Председатель Правления РНКО утверждает внутренний документ «Информация об обработке персональных данных в структурных подразделениях ООО РНКО "Металлург"», закрепляющий распределение функций по обработке персональных данных между структурными подразделениям РНКО.

6.2. В рамках каждого структурного подразделения РНКО выделяются сотрудники, ответственные как за организацию обработки персональных данных, так и сотрудники ответственные за обеспечение защиты персональных данных.

6.3. Лица, ответственные за организацию обработки и защиты персональных данных, получают указания непосредственно от Председателя Правления и подотчетны ему.

6.4. РНКО несет ответственность за неисполнение требований Закона «О персональных данных» в соответствии с действующим законодательством Российской Федерации.

6.5. Конкретные наказания за определенные действия/бездействие в области обработки персональных данных содержат нормы Кодекса Российской Федерации об административных правонарушениях и Уголовного кодекса Российской Федерации.

7 СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях защиты персональных данных, в РНКО, применяется комплекс документов в области стандартизации Банка России, требования национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», а так же иных актуальных нормативных актов Российской Федерации в части обеспечения безопасности информации персональных данных.

7.2. РНКО при обработке ПДн принимает 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. К таким мерам, в соответствии с Законом «О персональных данных» и ГОСТ 57580.1-2017, в частности, относятся:

- назначение лица, ответственного за организацию обработки ПДн, и лиц, ответственных за обеспечение безопасности ПДн;
- установление персональной ответственности работников РНКО за обеспечение безопасности обрабатываемых ПДн;
- определение угроз безопасности ПДн при их обработке;
- разработка и утверждение локальных актов по вопросам обработки и защиты ПДн;
- оценка вреда, который может быть причинен гражданам в случае нарушения Закона «О персональных данных», соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом «О персональных данных»;
- ознакомление работников РНКО, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами по вопросам обработки и защиты ПДн, и обучение работников РНКО;
- мониторинг изменений законодательства, нормативно-правовых и иных актов в сфере обработки и защиты ПДн, в том числе рекомендаций уполномоченного органа по защите прав субъектов ПДн, контролирующего деятельность РНКО по обеспечению безопасности ПДн, ознакомление со значимыми изменениями и указанными рекомендациями всех работников РНКО, непосредственно осуществляющих обработку ПДн, и приведение в соответствие с ними внутренних документов банка (в том числе регламентов, инструкций и т.д.);
- контроль выполнения подразделениями, должностными лицами и работниками РНКО требований законодательства, нормативно-правовых актов, настоящей политики и иных внутренних документов РНКО в области обработки и защиты ПДн, контроль соответствия обработки и защиты ПДн в РНКО указанным требованиям;
- классификация ПДн, ИСПДн (согласно требованиям законодательства);

- реализация принципа достаточности обрабатываемых ПДн (при определении состава обрабатываемых ПДн субъектов ПДн РНКО руководствуется минимально необходимым составом ПДн для достижения целей получения и обработки ПДн);
- соблюдение условий, исключающих несанкционированный доступ к материальным носителям ПДн и к средствам защиты ПДн;
- учет машинных носителей ПДн;
- хранение материальных носителей ПДн в закрытых шкафах, ящиках, сейфах;
- организация контроля доступа в помещения и здания банка, их охрана в рабочее и нерабочее время, ограничение доступа в помещения, где хранятся ПДн;
- содержание штата специалистов по защите информации, организация системы их профессиональной подготовки;
- организация и реализация системы ограничения (разграничения) доступа пользователей (обслуживающего персонала) к документам, информационным ресурсам и машинным носителям информации, информационным системам и связанным с их использованием работам;
- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- систематический анализ (мониторинг) безопасности ПДн, регулярные проверки и совершенствование системы их защиты;
- контроль и оценка эффективности принимаемых мер по обеспечению безопасности ПДн и уровня защищенности ИСПДн.
- применение технических мер защиты, включая:
- средства разграничения доступа на сетевом, прикладном и общесистемном уровнях;
- средства межсетевого экранирования;
- средства регистрации и учета действий пользователей на сетевом, прикладном и общесистемном уровнях;
- антивирусные средства защиты;
- сертифицированные средства криптографической защиты информации;
- средства обнаружения вторжений;
- средства анализа защищенности;
- средства контроля физического доступа в помещения, в которых осуществляется обработка ПДн.
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию новой информационной системы РНКО;
- 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 информационных системах РНКО, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн;
- осуществление внутреннего контроля и аудита соответствия обработки ПДн Закону «О персональных данных», ГОСТ 57580.1-2017 БС и подзаконным нормативным актам.

8 СПРАВОЧНАЯ ИНФОРМАЦИЯ

8.1. Контакты РНКО для обратной связи: адрес - 117292, г. Москва, ул. Ивана Бабушкина, 16А, телефон + 7 (495) 785-70-75

8.2. В случае направления официального запроса в РНКО, в тексте запроса необходимо указать:

- номер основного документа, удостоверяющего личность гражданина (или его законного представителя), сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие гражданина в отношениях с РНКО (например, номер и дата заключения договора, условное словесное обозначение) либо сведения, иным способом подтверждающие факт обработки ПДн РНКО;
- подпись гражданина (или его законного представителя). Если официальный запрос отправляется в электронном виде, то он должен быть оформлен в виде электронного документа и подписан электронной подписью в соответствии с законодательством РФ.