Утверждено приказом Генерального директора ООО «ЛЕО Фармасьютикал Продактс» № 3П-22 от 9.12.2022

Подпись _____

Галабурда Игорь Васильевич
Генеральный директор

Версия 1.0

Дата 09.12.2022

Approved by the order of the General Director of LEO Pharmaceutical Products LLC No 3P-22 of the 9th of December 2022

Signed _____

Igor V. Galaburda
General Director

Version 1.0

Date 09.12.2022

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общество с Ограниченной Ответственностью «ЛЕО Фармасьютикал Продактс»

POLICY ON PERSONAL DATA PROTECTION

"LEO Pharmaceutical Products" Limited Liability Company

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о защите персональных данных общества с ограниченной ответственностью «ЛЕО Фармасьютикал Продактс» (далее – Оператор или Общество разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории России.

1.2. Цель настоящего Положения – защита персональных данных субъектов персональных данных Общества от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

1.3. Настоящее Положение и изменения к нему утверждаются руководителем Общества. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1. GENERAL PROVISIONS

1.1. The Policy on Personal Data Protection of LEO Pharmaceutical Products Limited Liability Company (hereinafter referred to as the "Operator" or "Company") has been developed in accordance with Federal Law No. 152–FZ dated July 27, 2006 and other effective Russian regulatory legal acts on personal data protection.

1.2. This Policy aims at protection of personal data of the Company's personal data subjects from unauthorized access and disclosure, prevention and identification of violations of the Russian Federation legislation, and elimination of consequences of such violations.

1.3. This Policy and amendments thereto shall be approved by the Head of the Company. All employees must review and sign this Policy and amendments thereto.

1.4. В настоящем Положении используются следующие основные понятия:	1.4. The following basic terms are used in this Policy:
субъект персональных данных – физическое лицо (субъект персональных данных), данные которого передаются ООО «ЛЕО Фармасьютикал Продактс»	**personal data subject** is a natural person (personal data subject) whose data is transferred to LEO Pharmaceutical Products LLC;
персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)	**personal data** is any information related directly or indirectly to an identified or identifiable natural person (personal data subject);
Оператор - юридическое 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. В рамках данного Положения, оператором является ООО «ЛЕО Фармасьютикал Продактс»	**operator** is a legal entity that organizes and (or) performs personal data processing independently or jointly with others, as well as defines objectives of personal data processing, scope of personal data processing, actions (procedures) performed with personal data. Under this Policy, LEO Pharmaceutical Products LLC is the operator;
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;	**personal data processing** is any action (procedure) or complex of actions (procedures) performed with or without the use of automatic means on personal data, including collection, recording, classification, accumulation, storage, keeping current (updating, amendment), extraction, use, transfer (distribution, submission, access), depersonalization, blockage, deletion, destroyal of personal data;
согласие на обработку персональных данных – конкретные, предметное, информированное, сознательное и однозначное решение субъекта персональных данных о предоставлении его персональных данных для обработки оператору персональных данных;	**consent to the personal data processing** is a specific, substantive, informed, conscious and unambiguous decision of the personal data subject to provide their personal data for processing to the personal data operator;
автоматизированная обработка	**automatic personal data processing** is

персональных данных – обработка персональных данных с помощью средств вычислительной техники;

processing of personal data withe the use of computer equipment;

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

personal data submission means actions aimed at the disclosure of personal data to a certain person or a definite group of people;

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

personal data blockage is suspension of personal data processing (excluding cases where this processing is required to keep personal data current);

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;

personal data destroyal means actions that result in impossibility to recover the content of personal data in the personal data information system and (or) lead to destruction of personal data tangible media;

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

personal data depersonalization means actions that result in impossibility to identify personal data belonging to a certain personal data subject without additional information;

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

personal data information system is a set of personal data contained in databases and ensuring its information technologies and technical tools processing.

2. СПОСОБЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2. METHODS OF PERSONAL DATA PROTECTION

2.1. Оператор персональных данных для защиты персональных данных внедряет соответствующие технические и организационные меры для обеспечения надлежащего уровня защиты данных. Данное требование в наибольшей мере относится к компьютерному оборудованию (серверам и рабочим станциям), сетям и каналам коммуникаций, а также

2.1. To protect personal data, the personal data operator should implement appropriate technical and organizational measures to ensure an appropriate level of data protection. This requirement applies most to computer hardware (servers and workstations), networks and communication channels, as well as to applications; measures should be implemented as an element of the information security

приложениям; меры должны быть внедрены в качестве элемента системы управления информационной безопасностью. Обязательные меры, внедряемые для предотвращения неавторизованной обработки персональных данных, помимо прочего включают в себя средства контроля:

management system. Mandatory measures implemented to prevent unauthorized processing of personal data, include, but are not limited to, the following controls:

- физического доступа к системам обработки данных;
- physical access to data processing systems;
- логического доступа к системам обработки данных;
- logical access to data processing systems;
- ввода данных в системы обработки данных.
- data entry into data processing systems.

2.2. Оператором разработаны локальные акты, по вопросам обработки и защиты персональных данных.

2.2. The operator has developed local regulations on processing and protection of personal data.

2.3. Лица, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

2.3. Individuals directly engaged in the processing of personal data are familiar with the provisions of the Russian Federation legislation on personal data, including requirements for personal data protection, documents establishing policies for personal data processing, local regulations on personal data processing.

2.4. На сайте Общества опубликована политика в отношении обработки персональных данных.

2.4. The Company has published a policy on personal data processing on its website.

2.5. В Обществе назначен ответственный за организацию обработки персональных данных и ограничен и регламентирован состав работников, функциональные обязанности которых требуют конфиденциальных знаний.

2.5. The company has appointed a person responsible for arrangement of personal data processing, and has limited and regulated the number of employees whose functional duties require confidential information.

2.6. В Обществе присвоены персональные пароли для каждого рабочего места (конкретного работника) и рационально размещены рабочие места работников, при данном размещении исключается бесконтрольное использование защищаемой информации.

2.6. The company has assigned personal passwords for each workplace (specific employee) and efficiently placed employees' workplaces, thus excluding uncontrolled use of protected information.

2.7. В Обществе в наличии необходимые условия в помещении для работы с конфиденциальными документами и базами данных.

2.7. The company has necessary conditions in place on the premises for working with confidential documents and databases.

2.8. В Обществе обеспечивается учет машинных носителей персональных данных.

2.8. The company ensures accounting of machine-readable media for personal data.

2.9. В Обществе обеспечивается восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к правила доступа к персональным данным, информационной системе персональных данных, а также обеспечивается регистрация и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных.

2.9. The company ensures recovery of personal data modified or destroyed as a result of unauthorized access to personal data, the personal data information system, and also guarantees registration and accounting of all actions performed with personal data in the personal data information system.

2.10. В Обществе исключена возможность неконтролируемого проникновения или пребывания посторонних лиц в помещения, где ведется работа с персональными данными.

2.10. The company excludes a possibility of unauthorized access or presence of unauthorized persons at the premises where personal data is being processed.

2.11. В Обществе обеспечена сохранность носителей персональных данных и средств защиты информации.

2.11. The company ensures safety of media with personal data and data protection tools.

2.12. В Обществе применяются программно-технические средства, прошедшие в установленном порядке процедуру оценки соответствия.

2.12. The company uses software and hardware that have passed the established compliance assessment procedure

2.13. Лица, осуществляющие обработку персональных данных в Обществе без использования средств автоматизации, проинформированы об особенностях и правилах осуществления такой обработки, документами Общества установлены места хранения персональных данных и перечень лиц, осуществляющих обработку персональных данных.

2.13. Individuals who process personal data at the Company without the use of automatic tools are informed about specifics and rules of such processing; the Company’s documents establish places of personal data storage and the list of individuals involved in personal data processing.

2.14. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных

2.14. Written requests from other organizations and institutions within their competence and powers should be responded to in writing and to the extent allowing for non-disclosure of an excessive amount of personal information of personal data subjects.

сведений субъектов персональных данных.

3. СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

3.1. 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 Федерального закона «О персональных данных».

3.2. 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 Федерального закона «О персональных данных».

3.3. 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.

3.4. 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.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных

3. СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

3.1. Information protection tools for the personal data protection system should be chosen by the operator in accordance with regulations adopted by the Federal Security Service of the Russian Federation and the Federal Service for Technical and Export Control pursuant to Part 4 of Article 19 of the Federal Law “On Personal Data”.

3.2. During processing in the information system, personal data should be protected with the help of the personal data protection system neutralizing relevant threats identified in accordance with Part 5 of Article 19 of the Federal Law “On Personal Data”.

3.3. The personal data protection system should include organizational and (or) technical measures established with consideration to relevant threats to the security of personal data and information technologies used in information systems.

3.4. Relevant threats to personal data security mean a set of conditions and factors that create an actual danger of unauthorized access to personal data (including accidental access) during its processing in the information system, which may result in destroyal, modification, blockage, copying, provision, dissemination of personal data, as well as in other illegal actions.

Threats of the 1st type are relevant for the information system if, among other things, threats related to the presence of undocumented (undeclared) capabilities in the

(недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

system software used in the information system are relevant for it.

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.

Threats of the 2nd type are relevant for the information system if, among other things, threats related to the presence of undocumented (undeclared) capabilities in the application software used in the information system are relevant for it.

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.

Threats of the 3rd type are relevant for the information system if threats not related to the presence of undocumented (undeclared) capabilities in the system and application software used in the information system are relevant for it.

3.5. В компании определен 4й уровень защищенности персональных данных. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

3.5. The company has defined the 4th level of protection of personal data. The need to ensure the 4th level personal data protection during processing in the information system is established when at least one of the following conditions is present:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

a) threats of the 3rd type are relevant for the information system, and the information system processes publicly available personal data;

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.

b) threats of the 3rd type are relevant for the information system, and the information system processes other categories of personal data of the operator’s employees, or other categories of personal data for less than 100,000 personal data subjects who are not employees of the operator.

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

3.6. To ensure the 4th level personal data protection during processing in information systems, the following requirements must be met:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или

a) arrangement of security procedures on the premises where the information system is located, preventing a possibility of uncontrolled entry or presence of persons without the access rights on this premises;

пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

b) assurance of safety of media with personal data;

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

c) approval of the document establishing the list of persons whose access to personal data processed in the information system is necessary for performance of their official (job) duties by the operator's head;

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.

d) use of information protection tools that have passed the procedure for assessment of compliance with requirements of the legislation of the Russian Federation on information protection if use of such tools is necessary to neutralize relevant threats.

3.7. Контроль за выполнением требований, указанных в настоящем разделе, организуется и проводится Работодателем 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).

3.7. The Employer should, independently and (or) with involvement on a contractual basis of legal entities and individual entrepreneurs licensed to provide technical protection of confidential information, supervise fulfillment of the requirements specified in this section. This control should take place at least once every 3 years within periods established by the operator (authorized person).

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКА

4. ACCESS TO THE EMPLOYEE'S PERSONAL DATA

4.1. Внутренний доступ.

Право доступа к персональным данным имеют:

- Административный ассистент;
- Административный ассистент отдела продаж;
- Административный специалист;

4.1. Internal access

The following persons have access to personal data:

- Administrative Assistant;
- Sales Administrative Assistant;
- Administrative specialist;

- Генеральный директор;
- Заведующий складом организации оптовой торговли лекарственными средствами для медицинского применения;
- Менеджер по поиску оптимальных решений для пациентов
- Менеджер по управлению цифровыми каналами и комплаенс;
- Младший менеджер по поиску оптимальных решений для пациентов;
- работники бухгалтерии - к тем данным, которые необходимы для выполнения конкретных функций;
- Руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения) по согласованию с руководителем Работодателя;
- сам носитель данных.
- Старший менеджер по поиску оптимальных решений для пациентов;
- Старший специалист по работе с персоналом;
- при переводе из одного структурного подразделения в другое доступ к персональным данным работника может иметь руководитель нового подразделения по согласованию с руководителем Работодателя;

4.2. Внешний доступ.

Работодатель вправе осуществлять передачу персональных данных работника третьим лицам, в том числе в коммерческих целях, только с его предварительного

- General Director;
- Warehouse Manager;
- Patient Solutions Manager;
- Digital Customer Engagement and Compliance manager;
- Junior Patient Solutions Manager;
- accounting staff: to data required to perform specific functions;
- Managers of structural divisions depending on the field of activity (access to personal data of employees in their division only) provided approval of the Employer's head;
- data subject.
- Senior Patient Solutions Manager;
- HR and Payroll specialist;
- in case of transfer from one structural subdivision to another, the manager of the new subdivision may have access to the employee's personal data provided approval of the Employer's head;

4.2. External access

The employer may transfer the employee's personal data to third parties, including for commercial purposes, only with their prior written consent, except in cases when it is required to

письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных действующим законодательством Российской Федерации.

Перед передачей персональных данных субъектов, Общество должно предупредить третье лицо о том, что они могут быть использованы только в тех целях, для которых были сообщены. При этом у третьего лица необходимо получить подтверждение того, что такое требование будет им соблюдено.

Не требуется согласие работника на передачу персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в социальный фонд страхования России в объеме, предусмотренном действующим законодательством Российской Федерации (например, для сдачи отчетности СЗВ-М, СЗВ-ТД и др.);
- в налоговые органы;
- в военные комиссариаты;
- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства Работодателем;
- по мотивированному запросу органов прокуратуры;
- по мотивированному требованию правоохранительных органов и органов безопасности;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- по запросу суда;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным

prevent threats to the life and health of the employee, as well as in other cases established in the current legislation of the Russian Federation.

Before transferring the subjects' personal data, the Company should notify the third party that the data may be used only for the purposes for which they were submitted. Furthermore, the third party should confirm its compliance with this requirement.

The employee's consent is not required, if the personal data are transferred:

- to third parties in order to prevent threats to the life and health of the employee;
- to the Social Fund of the Russia in the scope established by the current legislation of the Russian Federation (i. e., when submitting the SZV-M, SZV-TD reports, etc.);
- to tax authorities;
- to military commissariats;
- at a request of employee representation bodies to monitor the Employer's compliance with the labor legislation;
- at a reasonable request of prosecution authorities;
- at a reasonable request of law enforcement and security agencies;
- at a request of state labor inspectors during their performance of supervisory and control activities;
- at a court's request;
- to agencies and organizations that must be notified of a serious accident, including a fatal one (in accordance with the Russian

исходом (в соответствии с законодательством Российской Федерации);

Federation legislation);

- в случаях, связанных с исполнением работником должностных обязанностей (согласно трудовому законодательству РФ).

- in cases related to performance of job duties by the employee (according to the labor legislation of the Russian Federation).

4.2.1. Обработка персональных данных иных субъектов персональных данных допускается в следующих случаях:

4.2.1. Processing of personal data of other personal data subjects is allowed in the following cases:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- processing of personal data is performed with a consent of the personal data subject given for processing of their personal data;

- обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

- personal data processing is necessary to achieve goals established by law, for implementation and fulfillment of functions, powers and duties assigned to the Operator by the Russian Federation legislation;

- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

- personal data is processed in connection with participation of the individual in constitutional, civil, administrative, criminal proceedings, or arbitration courts proceedings;

- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- personal data processing is required for execution of a judicial act, act of another agency or official to be executed under the Russian Federation legislation on enforcement proceedings;

- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в

- personal data processing is required for execution of powers of federal executive bodies, bodies of state extra-budgetary funds, state executive bodies of the Russian Federation subjects, local self-government bodies and functions of organizations involved in the provision of state and municipal services, provided for by Federal Law No. 210-FZ “On

предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

Provision of State and Municipal Services" dated July 27, 2010, respectively, including registration of the personal data subject in the unified portal of state and municipal services and (or) regional portals of state and municipal services;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;

- personal data processing is required for performance under a contract to which the personal data subject is a party, or beneficiary, or guarantor, as well as for execution of a contract by initiative of the personal data subject or a contract under which the personal data subject will a beneficiary or guarantor. A contract executed with the personal data subject cannot contain provisions restricting rights and freedoms of the personal data subject, establishing cases of personal data processing for minors, unless otherwise provided by the Russian Federation legislation, as well as provisions allowing inaction of the personal data subject as a condition precedent for the contract execution;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- personal data processing is required to protect the life, health or other vital interests of the personal data subject when it is impossible to obtain a consent of the personal data subject;

- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов

- personal data processing is required to exercise rights and legitimate interests of the operator or third parties, including cases established in the Federal Law "On Protection of Rights and Legitimate Interests of Natural Persons in Repayment

физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

of Overdue Debts and on Amendments to the Federal Law "On Microfinance Activities and Microfinance Organizations", or to achieve socially important purposes, provided that rights and freedoms of the personal data subject are not violated;

- в иных случаях, прописанных в законодательстве.

- in other cases prescribed by law.

4.3. Другие организации.

Сведения о работнике (в том числе уволенном) могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

Сведения о ином субъекте персональных данных предоставляются третьему лицу только с согласия данного субъекта (если иное не предусмотрено законодательством).

4.3. Other organizations

Information about an employee (including a dismissed one) may be provided to another organization only by a written request on the organization's letterhead with a copy of the employee's application attached.

Information about another personal data subject may be provided to a third party only by a consent of this subject (unless otherwise provided by law).

4.4. Родственники и члены семей.

Персональные данные работника и иных субъектов персональных данных могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника (иного субъекта персональных данных).

4.4. Relatives and family members

Personal data of an employee and other personal data subjects may be provided to relatives or family members only by the employee's (another personal data subject) own written permission.

5. ДОПОЛНИТЕЛЬНЫЕ ОБЯЗАННОСТИ ОПЕРАТОРА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5. OPERATOR'S ADDITIONAL OBLIGATIONS FOR PERSONAL DATA PROTECTION

5.1. Оператор обеспечивает взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

5.1. The operator should ensure interaction with the state system for detecting, preventing and eliminating consequences of computer attacks on the information resources of the Russian Federation, including notifying about computer incidents resulting in illegal transfer (provision, dissemination, access) of personal data.

5.2. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор обязан с момента выявления такого инцидента Оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение 24 часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение 72 часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5.2. If illegal or accidental transfer (provision, distribution, access) of personal data resulting in violation of the personal data subject rights is detected, the Operator must, from the moment when the Operator, authorized body for protection of personal data subject rights or another interested person detects such an accident, notify the authorized body for protection of personal data subject rights:

1) within 24 hours about the occurred incident, suspected causes of violation of personal data subject rights, and alleged harm caused to personal data subject rights, measures taken to eliminate consequences of the respective incident, as well as provide information about the person delegated by the operator to interact with the authorized body for protection of personal data subject rights on issues related to the detected incident;

2) within 72 hours about results of the internal investigation of the detected incident, and provide information about persons whose actions led to the detected incident (if any).

6. ОТВЕТСТВЕННОСТЬ

6.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

6. RESPONSIBILITY

6.1. Individuals violating regulations governing receipt, processing and protection of personal data of an employee are subject to disciplinary, administrative, civil or criminal liability in accordance with federal laws.