

УТВЕРЖДЕНА
Приказом Генерального директора
ПАО «ЭсЭфАй»
от 01.03.2023 г. № 003/1

Приложение № 1 к Приказу
от 01.03.2023 г. № 003/1

**ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ПУБЛИЧНОГО АКЦИОНЕРНОГО ОБЩЕСТВА «ЭсЭфАй»**

Москва
2023 год

Оглавление

1. Назначение и область действия.....	3
2. Определения документа.....	3
3. Цели и задачи.....	5
4. Роли и ответственность.....	5
5. Основные принципы и условия обработки персональных данных.....	7
6. Сведения о реализуемых требованиях к обеспечению безопасности ПДн.....	14
7. Права субъекта персональных данных.....	15
8. Порядок рассмотрения обращений субъекта ПДн.....	16
9. Заключение.....	18

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

1.1. С целью поддержания деловой репутации и обеспечения выполнения норм федерального законодательства, согласно требованиям Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Публичное акционерное общество «ЭсЭфАй», (далее Общество) определяет важнейшими задачами: обеспечение законности обработки персональных данных и обеспечение надлежащего уровня безопасности обрабатываемых в Обществе персональных данных.

1.2. Настоящий документ «Политика в отношении обработки персональных данных Публичного акционерного общества «ЭсЭфАй», (далее - Политика) направлен на определение общих принципов и условий Общества в области обработки персональных данных (далее - ПДн), формулировки целей и задач в данной области, определения отношений, связанных с обработкой ПДн, осуществляемых Обществом, распределения основных ролей и ответственности, и формализацию процесса управления защитой персональных данных в Обществе в рамках обеспечения соблюдения законодательства Российской Федерации. Настоящая Политика является документом второго уровня по отношению к Политике информационной безопасности ПАО «ЭсЭфАй» и определяет основные положения, реализуемые при обработке ПДн в Обществе, а также детализирует положения Политики информационной безопасности. Политика разработана в соответствии с законодательством РФ о ПДн и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн, в том числе при их обработке в информационных системах ПДн (далее - ИСПДн).

1.3. Областью действия документа являются действия, относящиеся к процессу управления защитой ПДн для всех процессов и информационных систем, относящихся к ИСПДн и все действия, связанные с обработкой (сбором, хранением, передачей, уничтожением и т.д.) ПДн. Настоящая Политика распространяется на всех работников Общества, осуществляющих обработку ПДн и обеспечивающих безопасность ПДн, а также является обязательным документом для исполнения всеми работниками Общества.

1.4. Настоящая Политика распространяется на все основные, обеспечивающие и управляющие бизнес-процессы Общества, а также технологические процессы, подпроцессы, процедуры и операции, в рамках которых осуществляется Обработка Персональных данных.

1.5. Действие настоящей политики не распространяется на отношения, возникающие при:

- Обработке Персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов Персональных данных;
- Организации хранения, комплектования, учета и использования содержащих Персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- Обработке Персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.6. Процесс управления защитой ПДн направлен на противодействие угрозам и уязвимостям, связанным с реализацией несанкционированного доступа с целью нарушения конфиденциальности или целостности ПДн, а также нарушения законных прав субъекта ПДн.

1.7. Требования настоящей Политики могут детализироваться, при необходимости, иными внутренними нормативными документами Общества.

2. ОПРЕДЕЛЕНИЯ ДОКУМЕНТА

2.1. Основные понятия, приведенные в настоящей Политике, полностью соответствуют понятиям, указанным в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее - ФЗ «О персональных данных»), а также в «Положении об

обработке и защите персональных данных работников ПАО «ЭсЭфАй». Термины и определения, специфические для данной Политики, указаны в разделе 2.2.

2.2. Термины, определения и сокращения:

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения 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.

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. В контексте данной политики ПАО «ЭсЭфАй»

Субъект персональных данных - физическое лицо, которое прямо или косвенно определено или определяется с использованием персональных данных.

Контрагент - физические лица, являющиеся представителями или работниками юридических лиц, состоящие в договорных отношениях или планирующие заключить договорные отношения с Обществом или физические лица, с которыми ПАО «ЭсЭфАй» состоит в договорных отношениях или намеревающиеся заключить с Обществом гражданско- правовые договоры, в том числе в связи с осуществлением хозяйственной деятельности Обществом.

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

Специальные категории персональных данных - данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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.

Общество – Публичное Акционерное Общество «ЭсЭфАй».

РКН - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации

РФ – Российская Федерация

ФЗ – Федеральный закон

ФЗ «О персональных данных» – Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»

3. ЦЕЛИ И ЗАДАЧИ

3.1. Основная цель разработки настоящего документа – определение политики Общества в отношении обработки ПДн и обеспечения безопасности ПДн.

3.2. Основной задачей Политики является определение высокоуровневых правил и требований к деятельности в области обработки и обеспечения безопасности ПДн.

4. РОЛИ И ОТВЕТСТВЕННОСТЬ

4.1. В рамках процесса обеспечения безопасности ПДн выделяются следующие роли:

– **Субъект ПДн** – физическое лицо, чьи ПДн обрабатываются Обществом и ПДн которого необходимо защищать.

– **Работник Общества, участвующий (допущенный) к обработке ПДн** – работник Общества, которому в рамках выполнения своих должностных обязанностей стали известны ПДн, обрабатываемые в Обществе, и который обеспечивает их конфиденциальность и безопасность.

– **Администратор ИСПДн** – работник Общества, который в рамках выполнения своих должностных обязанностей обслуживает, поддерживает и управляет требуемым составом технических средств, обеспечивающих обработку ПДн.

– **Куратор, ответственный за обеспечение безопасности ПДн** – руководитель подразделения безопасности, который в рамках выполнения своих должностных обязанностей осуществляет контроль за обеспечением выполнения требований в области обработки ПДн.

– **Ответственный за организацию обработки ПДн** – работник, ответственный за организацию процессов обработки и защиты ПДн, назначается Приказом Генерального директора Общества.

4.2. В должностных инструкциях работников Общества и соглашениях с третьими сторонами должны быть определены права и обязанности в соответствии с требованиями ФЗ «О персональных данных», для каждого участвующего в процессе обработки ПДн.

4.3. В случае нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Обществу, работникам и посетителям материального или иного ущерба виновные лица несут ответственность в соответствии с законодательством РФ:

- дисциплинарную, вплоть до расторжения трудового договора (ст. 81, 192 ТК РФ);
- административную (ст. 5.39, 13.11, 13.14 КоАП РФ);
- уголовную, при наличии состава преступления (ст. 137, 272 УК РФ).

5. ОСНОВНЫЕ ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Принципы обработки персональных данных

5.1.1. Обработка ПДн в Обществе осуществляется на основе следующих принципов:

- Общество осуществляет обработку ПДн с соблюдением принципов, правил и в случаях, предусмотренных ФЗ «О персональных данных», с учетом защиты интересов сторон процесса обработки;
- обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;
- не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только ПДн, которые отвечают целям их обработки;
- содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн.
- хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн;
- обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, в целях осуществления деятельности Общества не допускается.

5.2. Категории, состав и цели обработки персональных данных

5.2.1. В целях выполнения основной деятельности Общество обрабатывает ПДн субъектов, включая, но не ограничиваясь:

- физические лица, состоящие в договорных отношениях с Обществом или планирующие заключить договорные отношения (контрагенты, работники, в том числе бывшие работники и члены семей работников, кандидаты на замещение вакантных должностей);
- аффилированные лица Общества (акционеры, члены Совета директоров);
- физические лица, являющиеся представителями или работниками юридических лиц, состоящие в договорных отношениях или планирующие заключить договорные отношения с Обществом или физические лица, с которыми ПАО «ЭсЭфАй» состоит в договорных отношениях или планирует вступить в договорные отношения;
- посетители Общества.

Общество обрабатывает следующие категории персональных данных относительно каждой категории субъектов персональных данных в целях, указанных в таблице:

Категории субъектов ПДн	Цель обработки	Категория ПДн	Способ обработки ПДн
Контрагенты/и представители контрагента.	В целях осуществления деятельности Общества, в соответствии с уставом ПАО	ФИО, дата и место рождения, гражданство, место	Смешанный способ обработки

	<p>«ЭсЭфАй».</p> <p>Заключение/исполнение/изменение/расторжение договоров, в том числе для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем. Для достижения целей, предусмотренных федеральными законами РФ, для выполнения возложенных законодательством РФ на Общество функций, полномочий и обязанностей.</p>	<p>работы и должность, номер телефона, адрес электронной почты, адрес регистрации, данные документа, удостоверяющего личность.</p>	<p>(на бумажных/электронных носителях информации и в ИСПДн), с передачей по внутренней сети и с передачей по сети Интернет.</p>
<p>Работники/бывшие работники.</p> <p>Соискатели/Кандидаты на замещение вакантных должностей в Обществе.</p>	<p>В целях исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений. Заключение, сопровождение, изменение, расторжение трудовых договоров, которые являются основанием для возникновения или прекращения трудовых отношений между работниками и работодателем, в том числе исполнения работодателем обязательств, предусмотренных ФЗ, локальными нормативными актами, трудовыми договорами, иными нормативными правовыми актами, в том числе в целях ведения кадрового, воинского и бухгалтерского учета, составления налоговой отчетности.</p> <p>Оформление и страхование полисов (ДМС, страхование жизни, страхование от несчастных случаев).</p> <p>Оформление заявлений на выдачу зарплатных банковских карт.</p> <p>В целях принятия руководством Общества решения о приеме либо отказе в приеме на работу соискателей на замещение вакантных должностей в Обществе.</p>	<p>Ф.И.О. (при наличии), а также прежние Ф.И.О. (при наличии), дата, место и причина изменения (в случае изменения); пол; возраст, дата (число, месяц, год) и место рождения; фотографическое изображение; сведения о гражданстве; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; сведения, содержащиеся в страховом свидетельстве обязательного пенсионного страхования или документе (электронном документе), подтверждающем регистрацию в системе индивидуального (персонифицированного) учета; идентификационный номер налогоплательщика (ИНН); адрес и дата регистрации по месту жительства (месту пребывания), адрес</p>	<p>Смешанный способ обработки (на бумажных/электронных носителях информации и в ИСПДн), с передачей по внутренней сети и с передачей по сети Интернет.</p>

	<p>фактического проживания; номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи; реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения; сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения); сведения об образовании и (или) квалификации или наличии специальных знаний (в том числе наименование образовательной и (или) иной организации, год окончания, уровень образования, квалификация, реквизиты документа об образовании, обучении); информация о владении иностранными языками; сведения об отношении к воинской обязанности, о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документа, наименование органа, выдавшего его);</p>	
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

		<p> сведения о трудовой деятельности, а также информация о предыдущих местах работы, периодах и стаже работы; сведения, содержащиеся в документах, дающих право на пребывание и трудовую деятельность на территории РФ (для иностранных граждан, пребывающих в РФ); сведения, содержащиеся в разрешении на временное проживание в РФ (для иностранных граждан, временно проживающих в РФ), виде на жительство (для иностранных граждан, постоянно проживающих в РФ); сведения о доходах, обязательствах по исполнительным документам; номера лицевого счета, реквизиты банковской карты; сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (для отдельных категорий работников в случаях, предусмотренных законодательством); иные персональные данные, содержащиеся в документах, представление которых предусмотрено законодательством, </p>
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		если обработка этих данных соответствует цели обработки.	
Аффилированные лица Общества, члены Совета директоров. Кандидаты в Совет директоров Общества.	Выполнение обязанностей члена органа корпоративного управления Общества.	ФИО, дата и место рождения, гражданство, место работы и должность, адрес регистрации по месту жительства, номера домашнего, рабочего, мобильного телефонов, адрес электронной почты, фотография/изображение, данные документа, удостоверяющего личность, данные об образовании и квалификации, сведения о профессиональном опыте, сведения о владении акциями, долями в уставных капиталах ПАО «ЭсЭфАй» и иных юридических лиц, сведения об аффилированных лицах, сведения о судимости, должность занимаемая в органах управления иных юридических лиц. ИНН, номер страхового свидетельства обязательного пенсионного страхования	Смешанный способ обработки (на бумажных/электронных носителях информации и в ИСПДн), с передачей по внутренней сети и с передачей по сети Интернет.
Персональные данные в Обществе уничтожаются в следующих случаях	<ul style="list-style-type: none"> • В случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении целей обработки персональных данных; • По требованию субъекта персональных данных, если обрабатываемые в Обществе персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки; • В случае истечения срока хранения персональных данных; • В случае выявления неправомерной обработки персональных данных субъекта персональных данных, если обеспечить правомерность 		

	<p>обработки персональных данных невозможно;</p> <ul style="list-style-type: none"> • В случае отзыва субъектом персональных данных согласия на обработку его персональных данных (если персональные данные обрабатываются Обществом на основании согласия субъекта персональных данных); • В случае устранения причин, вследствие которых осуществлялась обработка персональных данных, если иное не установлено федеральным законом; • В случае ликвидации Общества.
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5.2.2. Цели и правовое основание обработки ПДн, состав и содержание ПДн, а также категории субъектов ПДн, чьи данные обрабатываются в Обществе, зафиксированы и подлежат обновлению в случае их изменения.

5.2.3. Состав ПДн должен соответствовать принципу их достаточности для достижения целей обработки. ПДн не должны быть избыточными по отношению к целям обработки.

5.3. Условия обработки персональных данных

5.3.1. Общество самостоятельно определяет состав, и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей по обработке ПДн, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральными законами.

5.3.2. Общество осуществляет обработку ПДн, как без использования средств автоматизации, так и автоматизированную обработку ПДн, с передачей и без передачи по внутренней корпоративной сети Общества, с передачей и без передачи в сети общего пользования Интернет.

5.3.3. Общество в ходе своей деятельности имеет право осуществлять трансграничную передачу ПДн на территорию иностранных государств органам власти иностранного государства, иностранным физическим или юридическим лицам. При этом вопросы обеспечения адекватной защиты прав субъектов ПДн и обеспечения безопасности их ПДн при трансграничной передаче являются наивысшим приоритетом для Общества, решение которых реализуется в соответствии с законодательством РФ по вопросам обработки ПДн.

5.3.4. В случае возникновения новых бизнес-процессов, предполагающих трансграничную передачу ПДн, до заключения договора с иностранным партнером (либо российским юридическим лицом, представляющим интересы иностранного партнера) необходимо получить от него сведения, касающиеся обработки ПДн, и направить уведомление в РКН о трансграничной передаче ПДн.

- После направления уведомления Общество вправе осуществлять трансграничную передачу персональных данных на территории указанных в таком уведомлении иностранных государств, которые являются сторонами Конвенции Совета Европы о защите физлиц при автоматизированной обработке персональных данных или включены в специальный Перечень, утвержденный Приказом Роскомнадзора от 05.08.2022 N 128. Это можно делать до принятия РКН решения о запрете или ограничении передачи данных.

- Общество не может до истечения установленных для рассмотрения уведомления сроков передавать персональные данные на территории указанных в уведомлении иностранных государств, которые не являются сторонами названной Конвенции Совета Европы и не включены в упомянутый Перечень. Исключение - ситуация, когда трансграничная передача необходима для защиты жизни, здоровья, иных жизненно важных интересов работника (других лиц).

5.3.5. Обработка ПДн Обществом осуществляется при наличии согласия в письменной форме субъекта ПДн в следующих случаях:

- для осуществления своей деятельности в соответствии с уставом ПАО «ЭсЭфАй», в том числе для заключения и исполнения договоров с контрагентами;
- для информационного обеспечения, создания общедоступных источников ПДн (телефонные справочники, адресные книги, размещаемые на корпоративном портале);
- для установления личности субъекта ПДн – при обработке сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн);
- для осуществления трансграничной передачи ПДн на территорию иностранных государств;
- для принятия решений на основании исключительно автоматизированной обработки ПДн.

5.3.6. Письменная форма согласия должна оформляться в соответствии с требованиями, предъявляемыми к ней ФЗ «О персональных данных».

Сроки обработки ПДн (сроки хранения) должны быть определены в соответствии с целями обработки ПДн и зафиксированы для каждой категории субъектов ПДн:

- по достижению целей обработки персональных данных или до момента утраты необходимости в достижении целей обработки персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных (если персональные данные обрабатываются Обществом на основании согласия субъекта персональных данных);
- в соответствии со сроками исковой давности, а также иными сроками, установленными законодательством РФ и нормативными документами.

5.3.7. Хранение ПДн должно осуществляться Обществом в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн. Сроки хранения также могут устанавливаться договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн, «Перечнем типовых управленческих документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», исковой давностью и иными требованиями законодательства, и нормативными документами.

5.3.8. Обработка ПДн может осуществляться без согласия субъекта ПДн в случаях, предусмотренных законодательством Российской Федерации.

5.4. Порядок и условия обработки ПДн

5.4.1. ПДн, обрабатываемые в Обществе, должны обладать уровнем конфиденциальности не ниже данных, отнесенных к Коммерческой тайне, а также к ним могут применяться и другие характеристики безопасности. В частности, к таким характеристикам относятся: целостность, доступность, неотказуемость, учетность (подконтрольность), аутентичность (достоверность), адекватность.

5.4.2. Общество реализует кадровую политику (тщательный подбор персонала и мотивация), позволяющую исключить или минимизировать возможность нарушения безопасности ПДн своими работниками.

5.4.3. Обработка ПДн в любой форме представления должна обеспечивать безопасность ПДн и определять информацию о методах и средствах обеспечения этой безопасности.

5.4.4. Предлагаемые меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы был результат их применения, мог быть измерен и оценен.

5.4.5. Неотъемлемой частью работ по защите ПДн должна являться оценка эффективности системы защиты ПДн.

5.4.6. С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн должны быть определены требования, мероприятия по обеспечению безопасности и процедуры для постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля должны регулярно анализироваться.

6. СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Общество для выполнения своих обязанностей, предусмотренных Федеральным законом «О персональных данных», для обеспечения безопасности и 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 принимает следующие правовые, организационные и технические меры:

- инвентаризация информационных систем ПДн, хранилищ и картотек, содержащих ПДн;
- оценка наличия основания для обработки ПДн каждой категории субъектов и каждой категории данных;
- назначение лица, ответственного за организацию обработки ПДн;
- корректировка бизнес-процессов, связанных с обработкой ПДн;
- определение актуальных угроз и уровня защищенности;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИС Общества;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации. При выборе средств защиты информации Общество руководствуется нормативными правовыми актами Регуляторов во исполнение части 4 статьи 19 Федерального закона «О персональных данных»;
- обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;
- обнаружение, предупреждение и ликвидация последствий компьютерных атак на информационные системы ПДн и реагирование на компьютерные инциденты в них;
- оператор обработки ПДн обязан уведомить РКН о факте(ах) неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшего(их) нарушение прав субъектов персональных данных, с момента выявления такого инцидента:
 - 24 часа – оповещение о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемой вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставление сведений о лице, уполномоченном оператором на взаимодействие с РКН, по вопросам, связанным с выявленным инцидентом;
 - 72 часа – оповещение о результатах внутреннего расследования выявленного инцидента, а также предоставление сведений о лицах, действия которых стали причиной выявленного инцидента (при наличии);
- оператор обработки ПДн в соответствии с установленными РКН требованиями должен оценить вред, который может быть причинен субъектам ПДн в случае нарушения законодательства по защите ПДн;
- регламентирование правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн;
- учет лиц, допущенных к обработке ПДн;
- учет машинных носителей ПДн;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн.

7. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОБЯЗАННОСТИ ОБЩЕСТВА

7.1. Субъект персональных данных имеет право:

- Отозвать согласие на обработку персональных данных посредством направления соответствующего письменного заявления в адрес Общества по адресу места нахождения. В этом случае Общество прекращает обработку персональных данных, а персональные данные подлежат уничтожению, если отсутствуют иные правовые основания для обработки, установленные законодательством Российской Федерации и/или документами Общества, регламентирующими вопросы обработки персональных данных.
- Отказаться от дачи согласия в любой форме, в том числе посредством прекращения использования сайта и/или отказаться от ввода персональных данных. В случае отказа в даче согласия это не создаст каких-либо юридических последствий в отношении субъекта персональных данных и не затронет права и законные интересы иным образом, но в таком случае субъекту известно, что это может повлиять на возможность оказания услуг или выполнения иных действий Обществом в интересах субъекта персональных данных.
- Получать от Общества сведения об обработке его персональных данных, включая право на получение информации, касающейся обработки его персональных данных, в том числе содержащей (право субъекта персональных данных на доступ к его персональным данным):
 - подтверждение факта обработки персональных данных субъекта Обществом, правовых оснований, целей и способов обработки персональных данных субъекта персональных данных;
 - наименование и место нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании федерального закона;
 - состав обрабатываемых Обществом персональных данных субъекта персональных данных, источник их получения;
 - сроки обработки Обществом персональных данных субъекта персональных данных, в том числе сроки их хранения;
 - информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
 - наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если такая обработка поручена или будет поручена такому лицу;
 - сведения о последствиях обработки Обществом персональных данных субъекта персональных данных.
- Требовать от Общества уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке действия или бездействия Компании, связанные с обработкой персональных данных субъекта персональных данных;
- Осуществлять защиту своих прав и законных интересов способами, установленными

законодательством Российской Федерации.

Право субъекта персональных данных на доступ к своим персональным данным может быть ограничено в соответствии с законодательством Российской Федерации.

7.2. Обязанности Общества при обработке персональных данных:

- Предоставлять субъекту по его запросу информацию, касающуюся обработки его персональных данных, либо на законных основаниях предоставить отказ в срок, не превышающий 10 (десяти) рабочих дней. Срок, может быть, продлен на 5 рабочих дней, если Общество направит в адрес субъекта мотивированное уведомление, в котором укажет причины отсрочки;
- По требованию субъекта ПДн уточнять обрабатываемые ПДн, блокировать или удалять,
- Если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки в срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих эти факты;
- Организовать прием, учет и обработку обращений и запросов субъектов персональных данных или их представителей, осуществляется контроль за приемом и обработкой таких обращений и запросов;
- В случае достижения цели обработки ПДн незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Обществом и субъектом ПДн, либо если Общество не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом N 152-ФЗ "О персональных данных" или другими федеральными законами;
- В случае отзыва субъектом ПДн согласия на обработку своих ПДн прекратить обработку ПДн, уничтожить ПДн и уведомить субъекта в срок, не превышающий 10 (десяти) дней;
- Обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных законодательством Российской Федерации;
- По запросу Роскомнадзора Общество должно предоставить необходимую информацию в течение 10 рабочих дней. При мотивированном уведомлении такой ответ можно продлить на 5 дней;
- Исполнять иные обязанности, установленные законодательством Российской Федерации.

8. ПОРЯДОК РАССМОТРЕНИЯ ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В случае получения Обществом обращений субъекта персональных данных (или его представителей) по вопросам обработки их персональных данных Обществом, в том числе обращения с требованием о прекращении обработки персональных данных, Общество осуществляет обработку обращения, готовит ответ субъекту персональных данных и обеспечивает прекращение обработки персональных данных в течение 10 (десяти) рабочих дней с момента получения такого обращения или запроса субъекта персональных данных. Срок предоставления ответа на обращение может быть продлен, но не более чем на 5 (пять)

рабочих дней, в таком случае Общество направляет в адрес субъекта персональных данных мотивированное уведомление с указанием причин продления срока.

Общество предоставляет ответ на запрос субъекта персональных данных в той форме, в которой направлено соответствующее обращение либо запрос, если иное не указано в обращении или запросе.

Если обращение в отношении персональных данных субъекта персональных данных получено от представителя субъекта персональных данных, Общество проверяет полномочия представителя субъекта персональных данных.

8.2. В случае выявления неправомерной обработки персональных данных субъекта персональных данных (персональные данные субъекта персональных данных являются незаконно полученными или не являются необходимыми для заявленной цели обработки), на основании сведений, предоставленных субъектом персональных данных (или его представителем) Общество в срок, не превышающий 3 (трех) рабочих дней с даты выявления указанного факта, блокирует персональные данные субъекта персональных данных на период проверки.

Общество обеспечивает правомерность обработки персональных данных. Если это невозможно, Общество в срок, не превышающий 10 (десяти) дней с даты выявления неправомерной обработки персональных данных субъекта персональных данных осуществляет уничтожение персональных данных в порядке, установленном настоящей Политикой.

Общество сообщает об устранении нарушений (неправомерной обработки персональных данных) или об уничтожении персональных данных субъекту персональных данных (или его представителю).

8.3. В случае выявления факта того, что персональные данные субъекта персональных данных являются неполными, устаревшими, неточными - на основании сведений, предоставленных субъектом персональных данных (или его представителем), если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц, Общество с момента обращения или получения запроса субъекта персональных данных блокирует персональные данные субъекта персональных данных. Если блокирование персональных данных нарушает права и законные интересы субъекта персональных данных или третьих лиц, Общество предоставляет субъекту персональных данных (или его представителю) соответствующее разъяснение.

Общество на основании сведений, предоставленных субъектом персональных данных (или его представителем), или иных необходимых документов уточняет персональные данные субъекта персональных данных в течение 7 (Семи) рабочих дней со дня предоставления субъектом персональных данных (или его представителем) сведений, на основании которых осуществляется уточнение персональных данных.

Уточнение персональных данных субъектов персональных данных при осуществлении их обработки без использования средств автоматизации производится Обществом путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными. Старый материальный носитель персональных данных уничтожается в порядке, установленном настоящей Политикой.

8.4. В случае запроса субъектом персональных данных (или его представителем), связанного с получением сведений, касающихся обработки персональных данных субъекта персональных данных, Общество в обязательном порядке осуществляет проверку следующих сведений (информации):

- запрос касается сведений об обработке персональных данных самого субъекта персональных данных, осуществившего запрос (или субъекта персональных данных, чьим представителем является лицо, осуществляющее запрос);
- запрос содержит информацию о номере основного документа, удостоверяющего личность субъекта персональных данных (или его представителя), информацию о дате выдачи указанного документа и выдавшем его органе, а также информацию, подтверждающую участие субъекта персональных данных в отношениях с Обществом

(номер договора, дата заключения договора, условное обозначение и/или иные сведения, либо сведения, иным образом подтверждающие факт обработки персональных данных субъекта персональных данных Обществом), подпись субъекта персональных данных (или его представителя);

- право субъекта персональных данных на доступ к его персональным данным не ограничено в соответствии с федеральными законами Российской Федерации.

Если одно, несколько или все указанные в настоящем пункте Политики условия не выполняются, Общество предоставляет субъекту персональных данных (или его представителю) соответствующее разъяснение, содержащее мотивированный отказ в предоставлении сведений, касающихся обработки его персональных данных в течение 10 (десяти) рабочих дней.

В случае выполнения всех указанных в настоящем пункте условий Общество предоставляет субъекту персональных данных (или его представителю) сведения, касающиеся обработки его персональных данных в срок в течение 10 (десяти) рабочих дней.

Если запрос субъекта персональных данных (или его представителя) является повторным, при этом сведения, касающиеся обработки персональных данных субъекта персональных данных, были предоставлены субъекту персональных данных (или его представителю) по его запросу, сделанному не ранее, чем за 30 (тридцать) дней до повторного запроса, то Общество предоставляет субъекту персональных данных (или его представителю) мотивированный отказ. Если повторный запрос осуществлен позднее, чем через 30 (тридцать) дней после предоставления субъекту персональных данных (или его представителю) сведений, касающихся обработки персональных данных субъекта персональных данных, по предыдущему запросу, то Общество предоставляет субъекту персональных данных (или его представителю) сведения, касающиеся обработки его персональных данных в срок, не превышающий 30 (тридцать) дней.

8.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных, Общество прекращает обработку персональных данных субъекта персональных данных, осуществляемую только на основании его согласия, если сохранение персональных данных субъекта персональных данных более не требуется для целей обработки персональных данных субъекта персональных данных.

Общество в срок, не превышающий 30 (тридцать) дней, осуществляет уничтожение персональных данных субъекта персональных данных, обрабатываемых только на основании его согласия и, если сохранение персональных данных субъекта персональных данных более не требуется для целей обработки персональных данных.

9. ЗАКЛЮЧЕНИЕ

9.1. Правовые основания обработки персональных данных:

Общество осуществляет обработку персональных данных субъектов персональных данных на следующих основаниях и в соответствии со следующими нормативными актами и документами:

- Федеральный закон Российской Федерации «О персональных данных» №152-ФЗ от 27 июля 2006 года;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 26.12.1995 N 208-ФЗ «Об акционерных обществах»;
- Устав ПАО «ЭсЭфАй»;
- Согласия субъекта персональных данных;
- Договор с субъектом персональных данных.
- Политика информационной безопасности ПАО «ЭсЭфАй».

Ответственность над реализацией настоящей частной политики лежит на Ответственном за организацию обработки ПДн.

Контроль за реализацией настоящей частной политики лежит на Кураторе, ответственном за обеспечение безопасности ПДн.

9.2. Настоящий документ будет регулярно пересматриваться – не реже 1 раза в 2 года либо при возникновении условий, оказывающих влияния на положения документа. Изменения в настоящую Политику могут вноситься в случаях изменения законодательства Российской Федерации о Персональных данных и принятых в соответствии с ним нормативных правовых актов, существенного изменения в структуре технологических и бизнес-процессов, в рамках которых осуществляется Обработка Персональных данных, изменения организационной структуры Общества, а также по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, по результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

9.3. В случае изменения законодательства Российской Федерации о Персональных данных и принятых в соответствии с ним нормативных правовых актов, изменения или введения в действие стандартов, нормативно-методических рекомендаций, требований уполномоченных органов настоящая Политика применяется в части, не противоречащей вновь принятым нормативным документам.

9.4. Внутренние нормативные и распорядительные документы Общества, затрагивающие вопросы Обработки и защиты Персональных данных, должны разрабатываться с учетом положений настоящей Политики и не противоречить им.

