

Положение
о процедурах, направленных на предотвращение и выявление нарушений
законодательства Российской Федерации, устранение последствий таких нарушений

1. Положение о процедурах, направленных на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений (далее – Положение) разработано в Обществе с ограниченной ответственностью «Сириус» (далее – Общество, Оператор) во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон).

2. Оператор осуществляет обработку персональных данных, основываясь на следующих принципах обработки:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей; обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается;
- объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой, не допускается;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки, а обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных; Оператор принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;
- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных; обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3. Оператором определены меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом, принятыми в соответствии с ним нормативными правовыми актами:

- назначено лицо, ответственное в Обществе за организацию обработки персональных данных;
- издан документ, определяющий политику Оператора в отношении обработки персональных данных, обеспечена возможность доступа к указанному документу с использованием средств информационно-телекоммуникационной сети «Интернет»;
- издан акт по вопросам обработки персональных данных, в котором для каждой цели обработки персональных данных определены категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, а также порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований;
- издан локальный акт, устанавливающий процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;
- определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;
- применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;
- произведен учет машинных носителей персональных данных;
- до ввода в эксплуатацию информационной системы персональных данных произведена оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;
- производится мониторинг обнаружения фактов несанкционированного доступа к персональным данным и принятие мер, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
- обеспечены средства для восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлены правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечены регистрация и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- производится контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных;
- осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных положениям Закона и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике в отношении обработки персональных данных, локальным актам Общества;

- осуществляется оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, соотношение причиненного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом;

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

4. Оператором обеспечивается 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 в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

5. К обязанностям Оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных, в частности, относятся следующие:

5.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу уполномоченного органа по защите прав субъектов персональных данных (далее – Роскомнадзор) Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, либо обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) – с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по его поручению, Оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по его поручению. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос Роскомнадзора были направлены Роскомнадзором, также уведомляет указанный орган.

5.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор блокирует персональные данные, относящиеся к этому субъекту персональных данных, либо обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) – с

момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) – в течение 7 (семи) рабочих дней со дня представления таких сведений и снимает блокировку персональных данных.

5.3. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор с момента выявления такого инцидента Оператором, Роскомнадзором или иным заинтересованным лицом, уведомляет Роскомнадзор:

- в течение 24 (двадцати четырех) 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 Роскомнадзором, по вопросам, связанным с выявленным инцидентом;

- в течение 72 (семидесяти двух) часов – о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Приложение № 1
к Положению о процедурах,
направленных на предотвращение и
выявление нарушений
законодательства Российской
Федерации, устранение последствий
таких нарушений

ЛИСТ ОЗНАКОМЛЕНИЯ

С Положением о процедурах, направленных на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, утв. _____ Общества с ограниченной ответственностью «Сириус» от «__» _____ 20__ г., ознакомлены:

№ п/п	Дата	ФИО	Должность	Подпись
1	2	3	4	5