

РЕГЛАМЕНТ
предоставления доступа к персональным данным в
ООО «Сатурн»

Москва 2018

Содержание

1	Информация о документе.....	3
1.1	Назначение документа	3
1.2	Цель принятия документа.....	3
1.3	Область применения документа.....	3
1.4	Вводимые сокращения и термины.....	3
1.5	Внешние нормативные и распорядительные документы	4
1.6	Внутренние нормативные и распорядительные документы	4
1.7	Пересмотр документа.....	4
2	Порядок предоставления допуска к обработке персональных данных.....	5
2.1	Допуск к обработке персональных данных работников Общества.....	5
2.2	Допуск к обработке персональных данных лиц, не являющихся работниками Общества.....	5
2.3	Инструктаж по правилам обработки и обеспечения безопасности персональных данных	6
3	Порядок предоставления доступа к информационным системам персональных данных.....	7
3.1	Предоставление прав доступа к информационным системам персональных данных.....	7
3.2	Изменение прав доступа к информационным системам персональных данных	7
3.3	Прекращение прав доступа к информационным системам персональных данных	8
3.4	Порядок рассмотрения и согласования Заявки на предоставление, изменение или прекращение прав доступа к ИСПДн	8
	Приложение № 1. Типовая форма соглашения о конфиденциальности работника	10
	Приложение № 2. Памятка о правилах обработки персональных данных	12
	Приложение № 3. Типовая форма соглашения о конфиденциальности физического лица	13
	Приложение № 3. Типовая форма журнала учета инструктажей по правилам обработки и обеспечения безопасности персональных данных	15
	Приложение № 5 Перечень структурных подразделений и должностей, допущенных к обработке персональных данных в ООО «Сатурн».....	17

1 Информация о документе

1.1 Назначение документа

1.1.1 Настоящий Регламент предоставления доступа к персональным данным в ООО «Сатурн» (далее – Регламент) определяет порядок предоставления работникам и третьим лицам доступа к персональным данным в ООО «Сатурн» (далее – Общество).

1.2 Цель принятия документа

1.2.1 Настоящий Регламент принят в целях обеспечения безопасности персональных данных при их обработке в Обществе.

1.3 Область применения документа

1.3.1 Настоящий документ обязаны знать и использовать в работе все работники Общества, допущенные к обработке персональных данных, а также Ответственный за обработку персональных данных и Ответственный за обеспечение безопасности персональных данных.

1.4 Вводимые сокращения и термины

Таблица 1 — Перечень сокращений

Сокращение	Расшифровка сокращения
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные

Таблица 2 — Перечень терминов

Термин	Определение термина
автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники
доступ к информации	возможность получения информации и ее использования
информационная система персональных данных	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
персональные данные	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

1.5 Внешние нормативные и распорядительные документы

Таблица 3 — Внешние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2	Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 24.07.2014) «О персональных данных»
3	Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
4	Приказ ФСТЭК России от 18.02.2014 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

1.6 Внутренние нормативные и распорядительные документы

Таблица 4 — Внутренние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Положение об организации обработки персональных данных
2	Положение об обеспечении безопасности персональных данных
3	Перечень структурных подразделений и должностей, допущенных к обработке персональных данных

1.7 Пересмотр документа

1.7.1 Пересмотр настоящего Регламента должен осуществляться в следующих случаях, но не реже одного раза в три года:

- при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;
- при существенном изменении процессов обработки персональных данных в Обществе.

2 Порядок предоставления допуска к обработке персональных данных

2.1 Допуск к обработке персональных данных работников Общества

2.1.1 К обработке персональных данных в Обществе допускаются работники, должности которых указаны в документе «Перечень структурных подразделений и должностей, допущенных к обработке персональных данных» (далее – Перечень) (Приложение № 6).

2.1.2 Предоставление допуска к обработке персональных данных работникам, должности которых не включены в Перечень, запрещено.

2.1.3 Допуск к обработке персональных данных предоставляется работнику Общества исключительно после выполнения следующих мероприятий:

а) подписания работником обязательства о неразглашении персональных данных (Типовая форма соглашения о конфиденциальности работника представлена в Приложении № 1);

б) ознакомления работника под роспись с внутренними нормативными и распорядительными документами в области обработки и обеспечения безопасности персональных данных;

в) прохождения работником инструктажа по правилам обработки и обеспечения безопасности персональных данных с внесением соответствующей записи в журнал инструктажей;

г) выдачи работнику экземпляра Памятки о правилах обработки персональных данных (Приложение № 2).

2.1.4 Обработка персональных данных, являющихся общедоступными (ФИО, должность, структурное подразделение, контактные данные), может осуществляться всеми работниками Общества без исключения и не требует включения работника в Перечень. Подписание обязательства о неразглашении персональных данных и прохождение инструктажа в данном случае не является обязательным.

2.2 Допуск к обработке персональных данных лиц, не являющихся работниками Общества

2.2.1 В случае, если допуск к обработке персональных данных необходимо предоставить лицам, не являющимся работниками Общества (физическим лицам, привлекаемым по договорам гражданско-правового характера, представителям контрагентов и т.п.), с таким лицом должно быть подписано соглашение о конфиденциальности. Типовая форма соглашения о конфиденциальности физического лица представлена в Приложении № 4.

2.2.2 Инструктаж и ознакомление с внутренними нормативными и распорядительными документами в области обработки и обеспечения безопасности

персональных данных в данном случае проводится по усмотрению Ответственного за обеспечение безопасности персональных данных.

2.2.3 Передача персональных данных другим юридическим лицам осуществляется в соответствии с документом «Регламент обмена персональных данных с третьими лицами».

2.3 Инструктаж по правилам обработки и обеспечения безопасности персональных данных

2.3.1 В Обществе проводятся первичные и периодические инструктажи по порядку обработки и обеспечения безопасности персональных данных.

2.3.2 Первичный инструктаж проводится при приеме (переводе) работника на должность, предполагающую допуск к обработке персональных данных, перед началом рабочей деятельности.

2.3.3 Периодический инструктаж проводится согласно утвержденному плану внутренних проверок состояния обработки и обеспечения безопасности персональных данных.

2.3.4 Организацию инструктажей осуществляет Ответственный за обработку персональных данных совместно с Ответственным за обеспечение безопасности персональных данных.

2.3.5 Инструктаж по порядку обработки и обеспечения безопасности персональных данных включает следующие темы:

- а) общие требования к порядку обработки персональных данных;
- б) правила обработки персональных данных в информационных системах Общества;
- в) правила неавтоматизированной обработки персональных данных (обработки бумажных носителей);
- г) правила использования средств антивирусной и парольной защиты, применяемых в Обществе;
- д) порядок действий при возникновении внештатных ситуаций;
- е) ответственность за нарушение правил обработки и обеспечения безопасности персональных данных.

2.3.6 Запись о проведенном инструктаже заносится в Журнал учёта инструктажей по правилам обработки и обеспечения безопасности персональных данных (далее – Журнал). Запись должна содержать:

- а) дату проведения инструктажа;
- б) Ф.И.О. и подпись лица, проводившего инструктаж;
- в) Ф.И.О. и подпись лица, прошедшего инструктаж.

2.3.7 Типовая форма Журнала приведена в Приложении № 4.

3 Порядок предоставления доступа к информационным системам персональных данных

3.1 Предоставление прав доступа к информационным системам персональных данных

3.1.1 Права доступа к ИСПДн предоставляется на постоянной или временной основе.

3.1.2 Права доступа к ИСПДн предоставляются работнику на основании Заявки на предоставление, изменение или прекращение прав доступа к ИСПДн (далее – Заявка) в соответствии с порядком, определенном в разделе 4.4 настоящего Регламента.

3.1.3 Доступ лиц к персональным данным в информационных системах персональных данных осуществляется после обязательного прохождения процедуры идентификации и аутентификации.

3.1.4 Процедура предоставления доступа работника к персональным данным в ИСПДн предусматривает:

- подачу непосредственным руководителем работника Заявки в соответствии с порядком, определенном в разделе 4.4 настоящего Регламента;
- уведомление непосредственного руководителя работника Администратором ИСПДн о результате ее исполнения;
- выдача работнику персонального идентификатора (логина) и первичного пароля. Пользователь должен сменить пароль при первом входе в ИСПДн.

3.2 Изменение прав доступа к информационным системам персональных данных

3.2.1 Основанием для изменения прав доступа работника к ИСПДн является:

- перевод работника на должность, в рамках структурного подразделения или Общества, функциональные обязанности которой требуют расширения или сокращения прав доступа к ПДн;
- изменение процесса (процессов) обработки ПДн в Обществе и/или требований законодательства РФ в области обработки и обеспечения безопасности ПДн, при которых расширяются или сокращаются права доступа к ПДн, закрепленные за определенными должностями работников;
- изменения в организационно-штатной структуре Общества;
- служебная необходимость, в рамках которой работнику требуется временное (разовое) расширение прав на обработку ПДн;
- проведение в отношении работника служебного расследования, в рамках которого такому работнику необходимо ограничить права доступа к ПДн.

3.2.2 Изменение прав доступа работника к персональным данным осуществляется на основании Заявки в соответствии с порядком, определенном в разделе 4.4 настоящего Регламента.

3.2.3 В случае изменений в процессе (процессах) обработки персональных данных или в организационно-штатной структуре Общества, соответствующие изменения должны быть внесены в документ «Перечень лиц, допущенных к обработке персональных данных в Обществе».

3.3 Прекращение прав доступа к информационным системам персональных данных

3.3.1 Основанием для прекращения прав доступа работника к ИСПДн является:

- нарушение работником требований организационно-распорядительной документации в области обработки и обеспечения безопасности ПДн;
- перевод работника на другую должность или в другое структурное подразделение, не требующих участия в процессах обработки ПДн;
- достижение заявленных целей, для которых работнику предоставлялся временный доступ к ИСПДн;
- прекращение трудовых отношений с работником.

3.3.2 Прекращение прав доступа работника к ИСПДн осуществляется на основании Заявки, направленной непосредственным руководителем работника в соответствии с порядком, определенном в разделе 4.4 настоящего Регламента.

3.4 Порядок рассмотрения и согласования Заявки на предоставление, изменение или прекращение прав доступа к ИСПДн

3.4.1 Предоставление, изменение или прекращение прав доступа работника к персональным данным осуществляется Администратором ИСПДн на основании Заявки непосредственного руководителя данного работника.

3.4.2 Под Администратором ИСПДн в настоящем регламенте понимается работник Общества, ответственный за эксплуатацию ИСПДн, в том числе за создание (изменение, удаление) учетных записей пользователей в ИСПДн.

3.4.3 Заявка подготавливается в виде служебной записки (документальной или электронной) и должна содержать:

- Ф.И.О. и должность работника, которому предоставляется доступ;
- наименование информационной системы, к которой необходимо предоставить доступ;
- основания для предоставления доступа;
- необходимые права доступа в системе (роль).

3.4.4 Срок выполнения Заявки должен быть минимальным, но не превышать 4-х рабочих дней, с момента ее получения Администратором ИСПДн.

3.4.6 Администратор ИСПДн уведомляет направившего Заявку о результате ее исполнения.

Приложение № 1. Типовая форма соглашения о конфиденциальности работника

Приложение
к трудовому договору № _____ от _____ г.

ОБЯЗАТЕЛЬСТВО (СОГЛАШЕНИЕ) О СОХРАНЕНИИ КОММЕРЧЕСКОЙ ТАЙНЫ И ИНОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Я, _____ (Ф.И.О.) (Далее – Работник), как лицо, состоящее в трудовых отношениях с ООО «Сатурн» (далее – Работодатель), осознаю, что в процессе работы получу доступ к информации Работодателя, в том числе к сведениям конфиденциального характера.

Я подтверждаю, что ознакомлен с Положением о режиме безопасности информации (конфиденциальности) Работодателя, утвержденным приказом Генерального директора ООО «Сатурн» № _____ от _____, в котором определены Перечень сведений, относимых к коммерческой тайне Работодателя и Перечень сведений, относимых к конфиденциальной информации Работодателя, порядок обращения с этой информацией и иные положения, касающиеся режима безопасности информации Работодателя.

Я подтверждаю, что не имею никаких обязательств перед каким-либо третьим лицом (физическим или юридическим), которые входят в противоречие с настоящим Обязательством или которые ограничивают мою деятельность на стороне Работодателя, и обязуюсь в период трудовых отношений с Работодателем (его правопреемником) и в течение 4-х лет после их окончания:

- не разглашать сведения, составляющие коммерческую тайну Работодателя, и иную конфиденциальную информацию, в том числе персональные данные, ставшую мне известной в процессе выполнения моих трудовых обязанностей;
- не передавать третьим лицам и не раскрывать публично сведения, составляющие коммерческую тайну Работодателя;
- выполнять требования локальных нормативных актов Работодателя по обеспечению защиты информации;
- в случае попытки посторонних лиц получить от меня защищаемые сведения немедленно сообщить об этом непосредственному руководителю и в Управление безопасности и режима Работодателя;
- сохранять ставшую мне известной в связи с трудовой деятельностью служебную тайну министерств и ведомств, а также коммерческую тайну тех контрагентов, с которыми у Работодателя имеются деловые (партнерские) отношения;

- не использовать коммерческую тайну и иную конфиденциальную информацию Работодателя для занятия любой деятельностью;
- в случае моего увольнения все носители коммерческой тайны Работодателя и иной конфиденциальной информации: рукописи, черновики, документы и т.д., которые находились в моем распоряжении в связи с исполнением трудовых обязанностей во время работы, передать по акту непосредственному руководителю;
- об утрате или недостатке носителей коммерческой тайны Работодателя и иной конфиденциальной информации, *удостоверений, пропусков, ключей*: от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению или утечке защищаемой информации, немедленно сообщить в Дирекцию Безопасности Работодателя.

Я согласен, что все конфиденциальные документы, подготовленные мной лично либо в сотрудничестве с другими лицами во время моей работы, будут являться собственностью Работодателя, и я сам не буду и не позволю никому делать копии, выдержки либо аннотации на вышеуказанные документы.

Я предупрежден о том, что в случае невыполнения мной любого из вышеперечисленных пунктов настоящего Обязательства и нарушения этих положений в отношении меня могут быть применены установленные законом меры ответственности, включая обязанность по возмещению Работодателю всех причиненных убытков.

Работодатель

Работник

_____ (подпись)

_____ (подпись)

«___» _____ 200__ г.

«___» _____ 200__ г.

_____ (должность)

_____ (Фамилия И.О.)

_____ (Фамилия Имя Отчество)

Приложение № 2. Памятка о правилах обработки персональных данных

1 Не разглашать персональные данные (далее - ПДн) других работников Общества и третьих лиц, ставшие известными при исполнении должностных обязанностей.

2 Не передавать обрабатываемые ПДн другим работникам Общества, не допущенным к обработке ПДн.

3 Не размещать в открытом доступе (корпоративные адресные книги, справочники, портал, сайты в сети Интернет и т.п.) ПДн работников Общества и третьих лиц, за исключением данных, признанных работниками общедоступными (Ф.И.О., должность, рабочий телефоны и e-mail, фотография, число, месяц и год рождения).

4 Перед началом обработки персональных данных убедиться в том, что:

а) рабочее место организовано способом, исключающим просмотр информации с бумажных (документальных) носителей ПДн, а также с дисплея рабочей станции посторонними лицами;

б) за время отсутствия на рабочем месте к персональной рабочей станции, информационной системе, сейфу или шкафу (ящику) не был осуществлен несанкционированный доступ;

в) средства обработки персональных данных находятся в исправном состоянии.

5 Выполнять требования по учету, хранению и уничтожению машинных и бумажных носителей персональных данных, в том числе не выносить носители персональных данных за пределы территории Общества без производственной необходимости.

6 После окончания рабочего дня убрать все носители персональных данных (флэшки, диски, бумажные документы и др.) в сейфы или запираемые металлические шкафы (ящики).

7 До начала передачи ПДн третьей стороне убедиться в том, что договор с третьей стороной содержит требования по обеспечению конфиденциальности передаваемых ПДн.

8 Хранить в тайне логины и пароли доступа к операционной системе и прикладным системам.

9 Использовать пароли доступа, отвечающие требованиям по безопасности (не использовать простые пароли), а также проводить периодическую смену пароля.

10 Незамедлительно оповестить своего непосредственного руководителя:

а) о ставших ему известными попытках разглашения ПДн, а также о других причинах или условиях возможной утечки ПДн;

б) в случае утери носителя персональных данных;

в) в случае обнаружения попыток несанкционированного доступа к рабочей станции, информационной системе, сейфу, шкафу и др.;

г) в случае отклонений от штатного функционирования, неустойчивой работы или выхода из строя технических компонентов информационных систем.

Приложение № 3. Типовая форма соглашения о конфиденциальности физического лица

Приложение № _____
к договору № _____ от _____ г.

ОБЯЗАТЕЛЬСТВО О СОХРАНЕНИИ КОММЕРЧЕСКОЙ ТАЙНЫ И ИНОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Я, _____ (Ф.И.О.) (далее – Исполнитель), как лицо, заключившее гражданско-правовой договор с ООО «Сатурн» (далее – _____), осознаю, что в процессе исполнения своих договорных обязательств получу доступ к информации Общества, в том числе к сведениям конфиденциального характера.

Я подтверждаю, что ознакомлен с Положением о режиме безопасности информации (конфиденциальности) Общества, утвержденным приказом Президента _____ № _____ от _____, в котором определены Перечень сведений, относимых к коммерческой тайне Общества и Перечень сведений, относимых к конфиденциальной информации Общества, порядок обращения с этой информацией и иные положения, касающиеся режима безопасности информации в Обществе.

Я подтверждаю, что не имею никаких обязательств перед каким-либо третьим лицом (физическим или юридическим), которые входят в противоречие с настоящим Обязательством или которые ограничивают мою деятельность на стороне Общества и обязуюсь в период гражданско-правовых отношений с Обществом (его правопреемником) и в течение 4-х лет после их окончания:

- не разглашать третьим лицам сведения, составляющие коммерческую тайну Общества, и иную конфиденциальную информацию, в том числе персональные данные, ставшую мне известной в процессе выполнения своих договорных обязательств без санкции Общества;
- не передавать третьим лицам и не раскрывать публично сведения, составляющие коммерческую тайну Общества;
- выполнять распоряжения Общества по обеспечению защиты информации;
- в случае попытки посторонних лиц получить от меня защищаемые сведения немедленно сообщить об этом в {Управление безопасности и режима} Общества;
- сохранять ставшую мне известной в связи с гражданско-правовыми отношениями служебную тайну министерств и ведомств, а также коммерческую тайну тех контрагентов, с которыми у Общества имеются деловые (партнерские) отношения;
- не использовать коммерческую тайну и иную конфиденциальную информацию Общества для занятия любой деятельностью;

- после прекращения гражданско-правовых отношений с Обществом все носители коммерческой тайны Общества и иной конфиденциальной информации: рукописи, черновики, документы и т.д., которые находились в моем распоряжении в связи с исполнением договорных обязательств перед Обществом, передать по акту в Управление безопасности и режима;
- об утрате или недостатке носителей коммерческой тайны Общества и иной конфиденциальной информации, *удостоверений, пропусков, ключей*: от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению или утечке защищаемой информации, немедленно сообщить в {Управление безопасности и режима}.

Я согласен, что все конфиденциальные документы, подготовленные мной лично либо в сотрудничестве с другими лицами во время исполнения договорных обязательств перед Обществом, будут являться собственностью Общества, и я сам не буду и не позволю никому делать копии, выдержки либо аннотации на вышеуказанные документы.

Я предупрежден о том, что в случае невыполнения мною любого из вышеперечисленных пунктов настоящего Обязательства и нарушения этих положений в отношении меня могут быть применены установленные законом меры ответственности, включая обязанность по возмещению Обществу всех причиненных убытков.

{Наименование юридического лица}

Исполнитель

_____ (подпись)

_____ (подпись)

«__» _____ 200__ г.

«__» _____ 200__ г.

_____ (должность)

_____ (Фамилия И.О.)

(Фамилия Имя Отчество)

Приложение № 3. Типовая форма журнала учета инструктажей по правилам обработки и обеспечения безопасности персональных данных

УТВЕРЖДАЮ

{Должность}
ООО «Сатурн»

_____ / _____

« ____ » _____ 2018 г.

ЖУРНАЛ

учёта инструктажей по правилам обработки и обеспечения безопасности персональных данных

Начат: « ____ » _____ 20 ____ г.

На ____ листах

Окончен: « ____ » _____ 20 ____ г.

(ФИО ответственного лица за ведение журнала)

подпись

Москва 2018

№ п/п	Дата инструктажа	Фамилия И.О., должность инструктирующего	Подпись	Фамилия И.О., должность инструктируемого	Подпись
1					
2					
4					
4					
6					
6					
7					
8					
9					
10					
11					
12					
14					
14					
16					
16					

**Приложение № 5 Перечень
структурных подразделений и должностей, допущенных к обработке
персональных данных в ООО «Сатурн»**

№ п/п	Наименование структурного подразделения	Должность	Информационные системы персональных данных, к которой предоставлен доступ
1	Дирекция по безопасности	Все сотрудники	<i>ИСПДн «Бухгалтерия и кадры»</i>
2	Департамент бухгалтерского и налогового учета и отчетности	Все сотрудники	<i>ИСПДн «Бухгалтерия и кадры»</i>
3	Юридический Департамент	Все сотрудники	<i>ИСПДн «Бухгалтерия и кадры»</i>
4	Департамент информационных технологий	Все сотрудники	<i>ИСПДн «Бухгалтерия и кадры»</i>
6	Департамент организационного развития	Все сотрудники	<i>ИСПДн «Бухгалтерия и кадры»</i>

В ООО «Сатурн» выделена информационная система персональных данных «Корпоративные ресурсы», являющаяся общедоступным источником персональных данных, к которой имеют доступ все работники ООО «Сатурн».