

Чек-лист для составления положения о персональных данных

1. Наименование оператора персональных данных (ООО, ИП?)
2. Адрес оператора персональных данных
3. Цели обработки персональных данных?
Например: с целью оказания услуг в сфере распространения компьютерных игр в сети Интернет, ведения кадровой работы и бухгалтерского учета.
4. Правовое основание обработки ПД?
Например: Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ; Налоговый кодекс РФ; Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», договоры с контрагентами (третьими лицами) на оказание услуг (при наличии), согласие на обработку персональных данных (при наличии), Устав ООО «_____» (если у вас ООО), федеральные законы по основному виду деятельности, предполагающие обработку персональных данных.
5. Какие персональные данные будут обрабатываться?
Например: фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; образование; профессия; доходы; СНИЛС, ИНН, стаж, данные документа, удостоверяющего личность?
Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Это могут быть также специальные категории персональных данных: расовая принадлежность, национальная принадлежность, политические взгляды, религиозные убеждения, философские убеждения, состояние здоровья, состояние интимной жизни.
Это могут быть также биометрические ПД: сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.
Cookie, IP-адреса тоже могут являться персональными данными!
6. Категории субъектов, персональные данные которых обрабатываются?
Например: работники, члены семьи работника, пользователи, иные лица.
7. Какие действия (совокупность действий) совершаются над персональными данными?
Например: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
8. Будет ли трансграничная передача персональных данных? Если да, то в какие страны?
9. Описание мер, предусмотренных статьями 18.1. и 19 Федерального закона «О персональных данных»:
Например: разработаны локальные акты по вопросам обработки персональных данных: положение об обработке персональных данных. Осуществляется внутренний контроль соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных. Работники, 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 организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных. Опубликован и размещен на стенде организации документ, определяющий политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Обеспечивается учет машинных носителей персональных данных. Обеспечивается восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним. Разработаны правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивается регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных

данных. Персональные данные доступны для строго определенного круга сотрудников, в здании установлены охранная и пожарная сигнализации, сведения на бумажных носителях хранятся в сейфах или запирающихся металлических шкафах, определены места хранения персональных данных, физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации; учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме).

10. Описать средства обеспечения безопасности.
Например: электронная цифровая подпись, используются антивирусные средства защиты информации, идентификация и проверка подлинности пользователя при входе в информационную систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов; наличие средств восстановления системы защиты персональных данных.
11. Описать сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.
Например: определены места хранения персональных данных (материальных носителей). Определен перечень лиц, осуществляющих обработку персональных данных и имеющих к ним доступ. Обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. Обеспечен учет материальных носителей. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, учтены в соответствующих журналах. Исключена возможность неконтролируемого проникновения или пребывания посторонних лиц в помещения, где ведется работа с персональными данными. Обеспечена сохранность носителей персональных данных и средств защиты информации.
12. Указать дату начала обработки персональных данных: _____
13. Каковы сроки или условия прекращения обработки персональных данных?
Например: прекращение деятельности ООО « _____ », ИП, иные основания.
14. Сведения об информационных системах, обрабатывающих ПД (их может быть несколько).
Например:

Сведения об информационной системе № 1:

Категории персональных данных

осуществляет обработку следующих категорий персональных данных:

фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; профессия; доходы;

а также: СНИЛС, ИНН, данные документа, удостоверяющего личность

Категории субъектов, персональные данные которых обрабатываются

принадлежащих: работников ООО « _____ », ИП, членов семьи работника

Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача, удаление

обработка вышеуказанных персональных данных будет осуществляться путем: автоматизированная/неавтоматизированная/смешанная; без передачи по внутренней сети

юридического лица/с передачей по внутренней сети юридического лица; без передачи по сети Интернет/с передачей по сети Интернет.

осуществление трансграничной передачи персональных данных: осуществляется (указать в какие страны)/не осуществляется

Сведения о местонахождении базы данных информации содержащей персональные данные граждан РФ:

Страна: Россия

Адрес ЦОДа:

Собственный ЦОД: есть/нет

Наименование организации (для ЦОД): ООО «_____»

организационно-правовая форма: общество с ограниченной ответственностью

адрес организации ЦОД: _____

ИНН: _____

ОГРН: _____

использование шифровальных (криптографических) средств: используются

наименование, регистрационные номера и производители используемых криптографических средств: _____

уровень криптографической защиты персональных данных:

15. Ответственный за организацию обработки персональных данных (может быть как физ.лицо, так и сторонняя организация): ФИО, почтовый адрес, номера контактных телефонов, адрес электронной почты.
16. ФИО исполнителя, должность, контактная информация исполнителя