



О процедуре обработки персональных данных при подключении сервиса распознавания документов

В соответствии с частью 3 статьи 6 Федерального закона РФ № 152-ФЗ «О персональных данных» оператор персональных данных вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

В связи с этим до заключения договора поручения на обработку персональных данных необходимо предпринять следующие действия:

1. Запросить полный комплект документов компании, предоставляющей сервис, включая, но не ограничиваясь учредительными документами, документами об обеспечении сохранности данных, имеющихся сертификатов и т. п.
2. Провести аудит компании-сервиса на предмет соблюдения требований безопасности обработки персональных данных. Федеральный закон РФ № 152-ФЗ «О персональных данных» таких обязанностей не содержит, но в случае обработки персональных данных иностранных граждан такой аудит носит обязательный характер (например, в силу Европейского GDPR).
3. Согласовать организационные и технические меры защиты между оператором и компанией-сервисом.
4. Внести во внутренние документы оператора, регламентирующие обработку персональных данных, изменения, касающиеся работы сервиса, в частности необходимо (ст. ст. 18, 18.1, 19 ФЗ «О персональных данных»):
 - 4.1 определить угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, внести изменения в модель (перечень) угроз утечки персональных данных;
 - 4.2 внести изменения в положение об обработке персональных данных, политику в отношении обработки персональных данных, инструкции и т. д.;
 - 4.3 указать во всей документации, имеющей отношение к бизнес-процессам, об автоматизированной обработке документов, содержащих персональные данные.
 - 4.4 в обязательном порядке о внесенных изменениях необходимо уведомить под роспись все сотрудников, отвечающих за обработку персональных данных.

5. В случае трансграничной передачи персональных данных оператору необходимо проводить индивидуальную оценку уровня защиты, предоставляемой для таких трансграничных передач, которая должна учитывать не только договорные положения, согласованные между сервисом и провайдером, но также и законы страны особенно те, которые касаются возможного доступа государственных органов этой страны к передаваемым персональным данным (ст. 12 ФЗ «О персональных данных»).

6. Получить от клиентов согласия на обработку персональных данных, включая информирование клиента об обработке персональных данных третьим лицом. В согласии должна быть указана цель обработки: распознавание документов для дальнейшей передачи третьим лицам. Форма согласия должна однозначно идентифицировать субъекта персональных данных. Примером такой формы согласия является письменная форма согласия (ст. 9 ФЗ «О персональных данных»)

7. Направить уведомление в Роскомнадзор об изменении способа обработки персональных данных, ИСПДн, средствах защиты, целей обработки персональных данных, трансграничной передачи. Такая необходимость возникнет в случае, если измененные внутренние документы будут содержать отличные от текущих сведений, имеющихся в Реестре операторов, осуществляющих обработку персональных данных (ч.7 ст. 22 ФЗ «О персональных данных»).

Необходимо иметь ввиду, что в случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор.

Таким образом, оператор остается ответственным за нарушения законодательства в обработке персональных данных (ч.5. ст. 6 ФЗ «О персональных данных»).

Ответственность за нарушение законодательства в области обработки персональных данных предусмотрена ст. 13.11 КоАП РФ, максимальный штраф по которой для юридических лиц достигает 6 000 000 рублей. Более серьезная ответственность наступает в случае нарушения правил GDPR, где максимальный штраф неограничен.

Перечень нормативных актов по обеспечению безопасности персональных данных

Специальные нормативные акты

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 19 декабря 2005 г. №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
- Федеральный закон от 7 мая 2013 г. №99-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона «О ратификации Конвенции Совета Европы О защите физических лиц при автоматизированной обработке персональных данных» и федерального закона "О персональных данных».
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
- Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ.
- Общее положение о защите данных (ЕС) 2016 /679 (GDPR)

Постановления Правительства РФ

- Постановление Правительства РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»
- Постановление Правительства от 19 августа 2015 г. № 857 «Об автоматизированной информационной системе «Реестр нарушителей прав субъектов персональных данных»

Ведомственные акты

- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».
- Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
- Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».
- Приказ Министерства связи и массовых коммуникаций РФ от 14 ноября 2011 г. № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных».
- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 15 марта 2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 15 февраля 2008 г.) .
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Федеральной службой по техническому и экспортному контролю 14 февраля 2008 г.

Разъяснения

- Разъяснения Роскомнадзора «О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки».
- Рекомендации по составлению политики обработки персональных данных (опубликованы на сайте Роскомнадзора).
- Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».
- Приказ Роскомнадзора от 22 июля 2015 г. № 85 «Об утверждении формы заявлений субъектов персональных данных о принятии мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных».
- Приказ Роскомнадзора от 22 июля 2015 г. № 84 «Об утверждении Порядка взаимодействия оператора реестра нарушителей прав субъектов персональных данных с провайдером хостинга и Порядка получения доступа к информации, содержащейся в реестре нарушителей прав субъектов персональных данных, оператором связи».

8 (800) 555-67-05
www.intellect.law

С уважением,
Михаил Хохолков
Ведущий юрист
m.hoholkov@intellectmail.ru