Hogan Lovells

Защита персональных данных в период пандемии

Наталья Гуляева

Управляющий партнер, глава практики интеллектуальной собственности, медиа и технологий Hogan Lovells CIS

Что такое персональные данные?

Персональные данные – любая информация, относящаяся к прямо или **косвенно** определенному или **определяемому** физическому лицу.

Персональные данные о состоянии здоровья относятся к специальным категориям персональных данных, к обработке которых предъявляются **дополнительные требования.**

Категории персональных данных

1. Специальные категории персональных данных
2. Биометрические персональные данные

→ Ограниченный перечень оснований обработки

3. Данные о судимости
4. Дактилоскопические данные

→ Обработка возможна только в случаях установленных законом

5. Данные работников

→ Для передачи третьим лицам необходимо письменное согласие

! Согласно текущей позиции Роскомнадзора, указание "да/нет" относительно вопроса о наличии судимости в анкете не подпадает под ограничения связанные с обработкой данных о судимости

Основания обработки персональных данных

Статья 6 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных":

1. согласие субъекта персональных данных

Наиболее универсальное и безопасное основание

2. достижение целей, предусмотренных международным договором или законом
3. участие лица в судопроизводстве
4. исполнение судебного акта или акта другого органа или должностного лица, подлежащего исполнению
5. исполнение полномочий органов государственной власти и местного самоуправления
6. осуществление прав и законных интересов оператора или третьих лиц

Согласие на обработку персональных данных

Требования к форме согласия:

1. Форма согласия должна позволять Оператору подтвердить факт его получения
2. Согласие должно быть предоставлено Субъектом ПДн свободно, своей волей и в своем интересе
3. Согласие на обработку персональных данных должно быть конкретным, **информированным и сознательным**

Согласие на обработку персональных данных

Примеры несоответствий:

1. Согласие потребителя на передачу ПДн третьим лицам, не охвачено самостоятельной волей и интересом потребителя, поскольку согласие потребителя, в данном случае, определено наличием поставленного символа "Х" в заявлении-анкете типографским способом, а не собственноручно .

2. Дополнительная строка для подписи под условием об обработке ПДн, помимо строки подписи под основными условиями заявления-анкеты отсутствует. Тем самым, ставя подпись в одном месте под заявлением-анкетой, потребитель подтверждает согласие со всеми условиями на данной странице заявления-анкеты, и соответственно при желании отказаться от какого-либо предложенного условия не может исключить эти условия из текста.

Дело № А40-172341/2018

Письменное согласие

Согласие в письменной форме должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок действия согласия, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

Письменное согласие: подпись

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается **согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью**.

Простая электронная подпись

Условия использования:

1. Соглашение между участниками
2. Правила применения ключа электронной подписи

Усиленная электронная подпись

1. Неквалифицированная
2. Квалифицированная

Обезличивание

Роскомнадзор

На сегодняшний день законодательство **не позволяет коммерческим организациям** осуществлять обезличивание персональных данных (за исключением обработки персональных данных в статистических целях).

Требования к обработке персональных данных **распространяются** на обезличенные данные.

Минкомсвязи уже разработан законопроект, который предлагает распространить существующие подходы к обезличиванию на деятельность коммерческих организаций.

Меры по обеспечению безопасности персональных данных

Оператор при обработке персональных данных обязан принимать необходимые:

1. **правовые меры**
2. **организационные меры**
3. **технические меры**

Персональные данные: правовые меры

1. **Принятие необходимых локальных актов, регулирующих процесс обработки персональных данных:**
   - Положение об обработке персональных данных,
   - Политика обработки персональных данных,
   - Положение о защите персональных данных и т.д.

2. **Обеспечение неограниченного доступа к политике по обработке персональных данных**

3. **Разработка типовых форм документов, касающихся обработки персональных данных** (согласия, анкеты и т.д.)

4. **Заключение договоров, регулирующих передачу персональных данных**

Дополнительно: Использование устройств компании и BYOD политика

- Использование работниками переносных устройств компании и устройств работника (смартфоны, планшеты, ноутбуки) увеличивает риски утечки информации
- Регулирование использования работником и компанией таких устройств необходимо для минимизации данных рисков:

- Для защиты информации и анализа действий с информацией компании на устройстве компании необходим доступ к устройству, используемому работником в работе
- Работник должен быть проинформирован, как устройство может быть использовано и как устройство использовать нельзя

Персональные данные: организационные меры

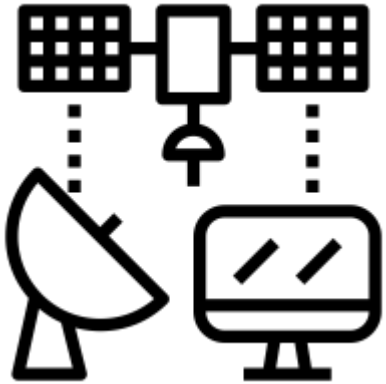
1. **Назначение ответственных лиц**
   - Ответственный за организацию обработки персональных данных,
   - Ответственный за обеспечение безопасности персональных данных
2. **Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения**
3. **Обеспечение локализации персональных данных**
4. **Ознакомление работников с порядком обработки персональных данных**
5. **Хранение материальных носителей в сейфах**
6. **Осуществление внутреннего контроля**
7. **Ограничение доступа к ИСПДн**

Персональные данные: технические меры

1. **Классификация ИСПДн**
2. **Определение угроз безопасности персональных данных**
3. **Определение необходимого уровня защищенности персональных данных**
4. **Обеспечение необходимого уровня защищенности персональных данных**

Дополнительно: Политика информационных технологий

- IT политика – "технический документ". Используемые технические меры защиты информации компании могут быть не формализованы в рамках IT политики
- Международные компании, как правило, стремятся к унификации и прозрачности в имплементации технических мер защиты информации, поэтому утверждают внутригрупповые IT политики
- Информирование рядовых работников о существовании и содержании IT политики не всегда необходимо. Сохранение такой политики в режиме конфиденциальности может быть необходимо в том числе и для целей защиты компании от киберрисков



COVID-19: Данные о здоровье работников

Температура тела относится к специальным категориям персональных данных. Следовательно, по общему правилу, для ее обработки требуется **письменное согласие лица, чья температура измеряется.**

В то же время, российское законодательство разрешает обработку данных о температуре тела без согласия субъекта персональных данных в следующих случаях:

1. Данная информация требуется для принятия решения о том, может ли работник выполнять свои должностные обязанности;
2. Сбор информации осуществляется без идентификации лиц, осуществляющих обследование.

Роскомнадзор рекомендовал рекомендовал ограничить срок обработки данных о температуре **одним днем.**

- Применимо ли данное разъяснение в более широком контексте и может ли применяться к иным ситуациям обработки данных **в публичных интересах?**
- Вправе ли работодатель принимать решения в отношении работников на основании данных, полученных при медицинском обследовании работников?

COVID-19: Личные устройства работников

Поскольку многие компании в связи с карантином перешли на удаленную работу, значительная часть работников стала использовать личные устройства в рабочих целях.

Игнорирование вопросов защиты персональных данных, связанных с использованием личных технических средств несет следующие риски:

1. Отсутствие возможности привлечь работника к ответственности в случае утечки конфиденциальной информации или несанкционированном доступа к устройству работника третьих лиц;

2. Отсутствие возможности доступа к бизнес-информации, хранящейся на личных устройствах работников;

3. Невозможность передачи данных, хранящихся на личных технических средствах работников, третьим лицам без согласия собственников таких средств.

COVID-19: Личные устройства работников

Шаги, которые необходимо предпринять для снижения рисков;:

1 **Разработка политики, регулирующей использование личных устройств (BYOD политики):**

- Политика должна устанавливать надлежащий порядок использования работником своего устройства за пределами офиса, включая необходимые защитные меры;
- Политика должна быть принята генеральным директором оператора данных;
- Все работники должны быть ознакомлены с политикой под собственноручную подпись.

2 **Согласие работников на обработку персональных данных:**

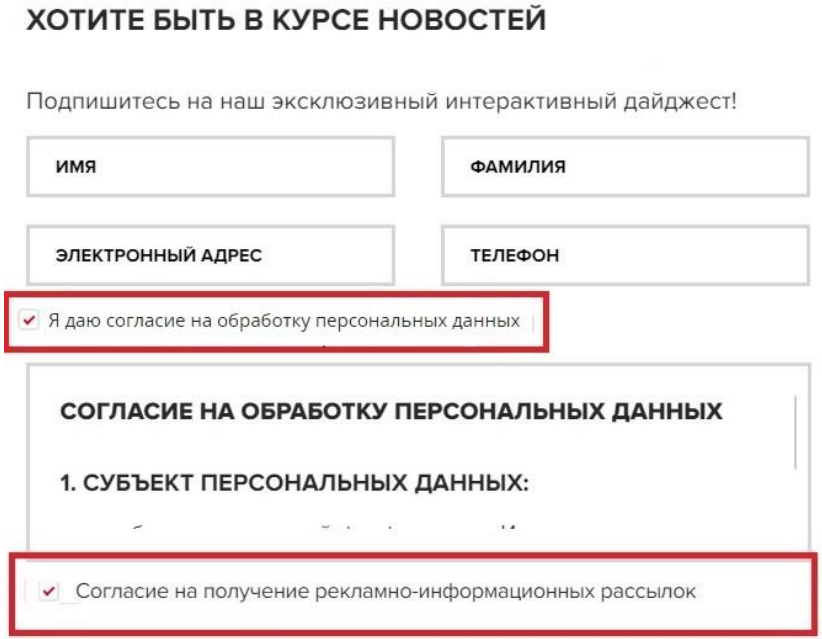
- Необходимо получить согласие работников на обработку их персональных данных, содержащихся на личных устройствах (для использования в целях обработки информации, относящейся к деятельности работодателя);
- Если доступ к персональным данным, находящимся на личных устройствах работников, может потребоваться по третьим лицам, например, головному офису, согласие работников должно быть предоставлено в письменной форме.

3 **Проведение тренингов по кибербезопасности для работников**

COVID-19: Продвижение

Обработка персональных данных с целью продвижения своих товаров и услуг клиентам: допускается, только если получено предварительное согласие на такую обработку от соответствующих субъектов персональных данных.

Согласно существующей правоприменительной практике, для целей продвижения своих товаров и услуг напрямую клиентам должно быть получено **отдельное согласие на обработку данных.**



Hogan Lovells

www.hoganlovells.com

All icons used in this presentation were taken from www.thenounproject.com