Вебинар

Персональные данные – актуальное 2025.
Разбираемся в поправках вместе с КонсультантПлюс.

КОМПАС ЛИДЕРА

8 (812) 320-44-22 info@compaslidera.ru compaslidera.ru

СОДЕРЖАНИЕ

- ✓ Работодатель и персональные данные работников – обязанности и требования;
- ✓ Виды и категории персональных данных;
- ✓ Согласие на обработку и распространение ПД - особенности;
- ✓ Уведомление Роскомнадзора;
- ✓ Проверки Роскомнадзора – на что обратить внимание?
- ✓ Обезличивание персональных данных.

КОМПАС ЛИДЕРА

Персональные данные -

любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному или определяемому физическому лицу (ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»

Собираются и обрабатываются как в отношениях

Работодатель-работник,

так и в отношениях

Поставщик товаров(услуг) –клиент.

Персональные данные – использование работодателем.

В главе 14 Трудового кодекса РФ раскрывается понятие ПД работника. Это данные, которые позволяют получить определенные характеристики человека в качестве сотрудника конкретной компании (стаж работы, профессиональная квалификация, заработная плата, данные по ФНС, СФР и пр.)

Они должны храниться должным образом и применяться для того, чтобы помочь работнику выполнять его обязанности в соответствии с его должностью и профессией, повышать свою квалификацию и получать новые профессиональные знания, и используются с целью защиты сотрудников и имущества компании.

Целью, которую преследует обработка и хранение ПД на предприятии, является необходимость правильно реализовать рабочую активность компании. Обработка ПД необходима для:

- ✓ фиксации факта приема сотрудника на работу;
- ✓ удостоверения оснований для продвижения по карьерной лестнице;
- ✓ подтверждения оснований для выплаты зарплаты;
- ✓ осуществления контроля выполнения производственных заданий и работ.

Работникам должна быть доступна информация о том, как осуществляется хранение и обработка их личных данных, поэтому наниматель обязан ознакомить их с данной информацией.

Основные обязанности работодателя, которые он должен исполнять при работе с персональными данными:

- ✓ разработать и принять ЛНА, регламентирующие порядок работы с персональными данными работников;
- ✓ назначить лицо, ответственное за организацию обработки персональных данных;
- ✓ установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- ✓ установить перечень мест хранения документации с ПД, перечень мер для обеспечения их сохранности;
- ✓ ознакомить работников под подпись с положением о ПД;
- ✓ брать письменное согласие, которое должно быть конкретным, информированным, содержать четкий объем ПД, а также согласие для передачи своих персональных данных третьим лицам с указанием этих лиц;

Работодателю необходимо собрать два типа ПД:

- ✓ требуемых для заключения трудового договора;
- ✓ запрашиваемых и формируемых непосредственно работодателем.
- ✓ ПД, которые хранятся на предприятии в личных делах по каждому работнику, обычно содержат данные:
- ✓ о семейном статусе и отдельных членах семьи (иждивенцы, дети, возрастные данные, количество, данные о состоянии здоровья и др.);
- ✓ копии документов по пенсионному государственному страхованию;
- ✓ о конкретном сотруднике (паспортные данные, профессия, квалификационные характеристики и др.).

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ.

Если вы получаете, храните, используете или совершаете иные действия с персональными данными граждан, это признается их обработкой, а вы - **оператором.**

Обработкой персональных данных **считаются любые действия или операции, которые вы проводите с ними, в том числе сбор, систематизация, хранение, уточнение, использование, распространение, удаление**.

Так, даже если вы, например, всего лишь получаете паспортные данные клиентов или создали базу данных их телефонных номеров, вы обрабатываете персональные данные и признаетесь их оператором.

До начала обработки данных вам нужно определить ее цель. Это важно, поскольку обработка должна соответствовать этой цели. В частности, вы не можете запрашивать данные, не связанные с этой целью. Например, получать у лица, с которым вы заключаете договор, персональные данные членов его семьи.

Если вы используете персональные данные граждан только для заключения и исполнения договоров с ними и никому их не передаете, то вам не нужно получать согласие гражданина на обработку данных и уведомлять о ней Роскомнадзор.

Работодатель является оператором персональных данных (ПД) своих работников. Не забудьте подать уведомление об обработке ПД в Роскомнадзор!

Какими способами можно обрабатывать персональные данные?

Вы можете обрабатывать данные **с использованием или без использования средств автоматизации** (п. 3 ст. 3 Закона о персональных данных).

Автоматизированной считается обработка данных с помощью средств вычислительной техники. **Обработкой без применения средств автоматизации** считаются действия с персональными данными, которые осуществляются при непосредственном участии человека (п. 4 ст. 3 Закона о персональных данных, п. 1 Положения, утвержденного Постановлением Правительства РФ от 15.09.2008 N 687).

Обработка ПД БЕЗ средств автоматизации.

В настоящее время действует ПОЛОЖЕНИЕ об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации(утв. **Постановлением Правительства РФ от 15.09.2008 N 687**.)

Согласно этому ПОЛОЖЕНИЮ обработкой ПД без применения средств автоматизации считаются использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются **при непосредственном участии человека** (п. 1 Положения)

Как организовать защиту персональных данных работников при обработке этих данных, если они хранятся на бумажных носителях?

Требования к организации защиты персональных данных на бумажных носителях (неавтоматизированная обработка) подробно не описаны в законе.

Ключевое требование закона – нужно принимать правовые, организационные и технические меры для защиты персональных данных работников от неправомерного использования или утраты либо обеспечить принятие таких мер (п. 7 ст. 86 ТК РФ, ч. 1 ст. 19 Закона о персональных данных).

Поэтому рекомендуется, в частности, следующее:

- ✓ хранить персональные данные на бумажных носителях в специальных помещениях. Учитывайте, что нужно раздельно хранить персональные данные (материальные носители), которые обрабатываются в разных целях (п. 14 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации);

- ✓ организовать особый режим доступа в эти помещения, в частности утвердить перечень лиц, имеющих доступ в данные помещения с учетом требований п. 13 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации;

- ✓ организовать охрану таких помещений, например оборудовать их сигнализацией, металлическими самозакрывающимися дверьми, решетками на окнах.

- ✓ Обратите внимание, что в некоторых случаях обязательно хранить персональные данные в железных шкафах. Например, в таких шкафах должны храниться документы воинского учета, содержащие персональные данные работников (п. 21 Методических рекомендаций по ведению воинского учета в организациях).

  Воспользуйтесь Готовым решением: **Какие меры по защите персональных данных работников должны приниматься при обработке этих данных (2025).**

Автоматизированная обработка ПД.

Автоматизированной считается обработка данных с помощью средств вычислительной техники.

Средства автоматизации, используемые при обработке персональных данных - это средства вычислительной техники. Это следует из определения автоматизированной обработки персональных данных как обработки с помощью средств вычислительной техники (п. 4 ст. 3 Закона о персональных данных). Под средствами вычислительной техники понимается неразделимая совокупность аппаратных и программных средств, предназначенная для выполнения определенного набора функций самостоятельно или в составе других систем (разд. 1 ГОСТ Р 71784-2024).

Конкретный перечень средств автоматизации, используемых при обработке персональных данных, законодательством РФ не определен. На практике обработкой с использованием таких средств может являться, например, обработка персональных данных с помощью информационных систем, в которых персональные данные формируются в виде отчетности в требуемых форматах автоматически путем внесения соответствующих персональных данных, извлекаемых из базы данных.

По общему правилу не допускаются запись, систематизация, накопление, хранение, уточнение, извлечение персональных данных граждан РФ с использованием баз данных, находящихся за пределами территории РФ. Это касается также сбора данных через Интернет (ч. 5 ст. 18 Закона о персональных данных).

ВИДЫ и КАТЕГОРИИ персональных данных.

Существует условное деление на **ОБЩИЕ(обыкновенные), СПЕЦИАЛЬНЫЕ, БИОМЕТРИЧЕСКИЕ, ПД разрешенные субъектом для распространения, ОБЕЗЛИЧЕННЫЕ** категории персональных данных.

Такое деление важно знать для осуществления правильного подхода к обработке и защите персональных данных. Происходит так потому, что некоторые категории ПД накладывают достаточно жесткие требования на оператора:

- ✓ обязательное наличие письменного согласия,
- ✓ обработка строго на основании правовой нормы,
- ✓ особый подход к методам защиты ПД.

- ✓ **ОБЩИЕ** – из толкования п. 1 ст. 3, ч. 1 ст. 10 и ч. 1 ст. 11 152-ФЗ следует вывод о том, что к ПД общей категории относятся такие сведения о субъекте, которые содержат информацию о нем, позволяющую его идентифицировать, но при этом не отнесенные законом к специальным категориям.

Например, к ПД общей категории могут быть отнесены фамилия, имя, отчество, дата, место рождения, пол, адрес места жительства или места пребывания, гражданство или отсутствие гражданства, реквизиты документа, удостоверяющего личность, СНИЛС, ИНН, персональные данные родственников, законных представителей субъекта, сведения о его образовании, месте работы, социальном положении, доходах и т.п.;

- ✓ **СПЕЦИАЛЬНЫЕ** - информация о личности человека, в частности расовая и национальная принадлежность, политические, религиозные и философские взгляды, состояние здоровья, подробности интимной жизни, информация о судимостях (ч.1, ч.3 ст.11 Закона о персональных данных).

Специальные категории персональных данных отличаются от общих тем, что **обычно находятся в закрытом доступе**. Их можно узнать только лично у человека, либо сделав официальный запрос в больницу, полицию или суд. Чаще всего сообщать эти данные человек не обязан, они — его личное дело.

Сбор, обработка и хранение таких ПД осуществляется с огромным количеством запретов.

Если вы в обработке столкнулись с чем-то подобным, сразу же возникают ограничения на правовые основания обработки этих данных, которые вы можете увидеть в ст. 10 Закона N 152-ФЗ.

Наиболее жесткие ограничения – для сведений о судимости (п. 3 ст. 10 Закона N 152-ФЗ). **Даже при наличии письменного согласия коммерческая компания не сможет обрабатывать такие сведения**. Зато их возможно обрабатывать в случаях, установленных законодательством. Например, сведения о судимости могут быть правомерно обработаны, если законодательство требует проверить наличие или отсутствие судимости при приеме не работу работника на определенную должность.

- ✓ **БИОМЕТРИЧЕСКИЕ персональные данные -** это такие сведения о физиологических и биологических особенностях человека, по которым можно установить его личность (ч. 1 ст. 11 Закона о персональных данных).

Какие именно сведения являются биометрическими персональными данными, Закон о персональных данных не определяет. Конкретного исчерпывающего перечня таких сведений нет и в нормативных документах.

Обратимся к Письмам Минцифры России от 17.07.2020 N ОП-П24-070-19433 и Роскомнадзора от 10.02.2020 N 08АП-6782 – они могут помочь понять суть и смысл данной категории персональных данных.

Как правило, к биометрическим персональным данным относят, например:

- ✓ фотографическое изображение человека;
- ✓ видеоизображение человека;
- ✓ дактилоскопические данные;
- ✓ информация о радужной оболочке глаза;
- ✓ результаты анализов ДНК;
- ✓ данные о голосе.

Если фото вы используете для установления личности человека, оно признается биометрическими ПД. Например, к биометрическим ПД относят фото на пропуск, так как сравнивая фото с лицом предъявителя пропуска, вы можете установить его личность (ч. 1 ст. 11 Закона о персональных данных, **Письмо Минцифры России от 17.07.2020 N ОП-П24-070-19433**).

Фото – особенности размещения с точки зрения конфиденциальности и нарушения норма 152-ФЗ.

Стоит отметить, что изображение человека в некоторых случаях относится к его персональным данным, а значит, использование фотографий граждан (в том числе несовершеннолетних) регулируется нормами закона.

По общему правилу, если фотографическое изображение вы используете для установления личности человека, оно признается биометрическими персональными данными. Например, к биометрическим персональным данным относят фото на пропуск, так как, в частности, сравнивая фото с лицом предъявителя пропуска, вы можете установить его личность (ч. 1 ст. 11 Закона о персональных данных, **Письмо Минцифры России от 17.07.2020 N ОП-П24-070-19433**).

Таким образом, **отнесение фотографии, например, публичного мероприятия к персональным данным зависит от цели обработки такой информации.**

Если оператор использует изображение для идентификации лица, то оно будет рассматриваться в качестве биометрических персональных данных по ч. 1 ст. 11 закона №152-ФЗ.

Если же такой цели нет, изображение не содержит других относимых к персоне сведений, получено при проведении публичного мероприятия, не является основным объектом использования и не предназначено для идентификации изображённого лица, то такая фотография или видеозапись не рассматривается в качестве персональных данных.

А значит, если изображение работника, полученное при проведении корпоратива, фото во время проведения общественных мероприятий (в том числе и несовершеннолетних – в школах, детских садах, библиотеках) не используется в целях его идентификации, не обрабатывается совместно с иными сведениями о нём и не является основным объектом использования, то это не будет признаваться персональными данными, и согласие не нужно.

Если же планируется размещение на сайте изображения работника с дополнительной информацией о нём, то такая фотография или видеозапись будут считаться персональными данными и потребуют получения от него отдельного согласия на распространение

Охрана изображения гражданина защищена статьей 152.1 Гражданского кодекса РФ, которая гласит, что обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен), если они являются ПД, допускаются только с согласия этого гражданина.

Такое согласие не требуется в случаях:

- ✓ Использование изображения осуществляется в государственных, общественных или иных публичных интересах;
- ✓ Изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях.

Например, это может быть на собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях, за исключением случаев, когда такое изображение является основным объектом использования;

- ✓ Гражданин позировал за плату.

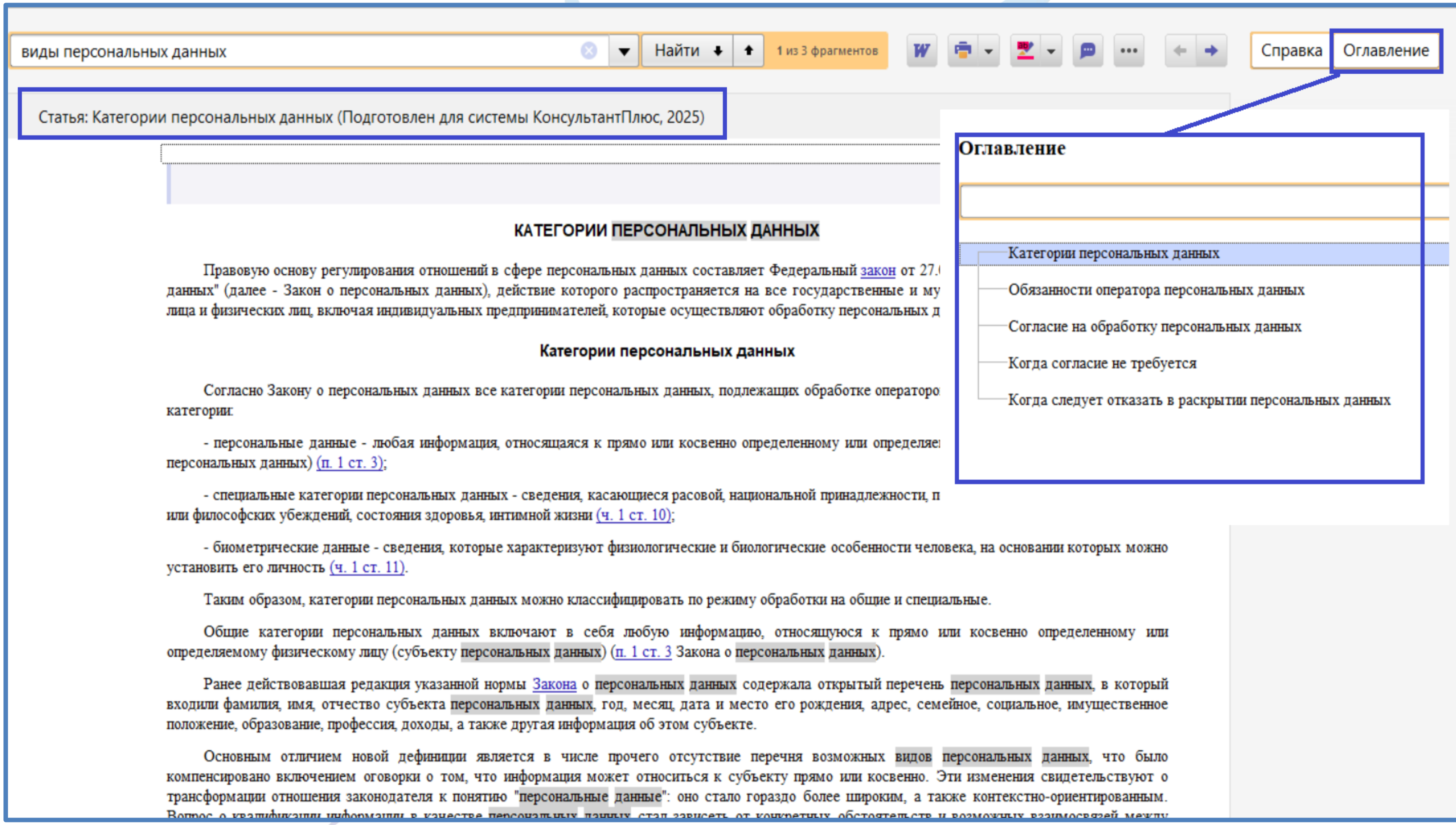
Если фото было опубликовано без согласия в Интернете, то субъект вправе обратиться с жалобой в прокуратуру на нарушение их прав, предусмотренных статьей 24 Конституции и статьей 152.1 ГК РФ. В случае, если публикация фотографий причинила ребенку (или его законным представителям) нравственные страдания, родители вправе обратиться в суд с иском о возмещении морального вреда, причиненного незаконным использованием изображения гражданина.

Специальные и биометрические персональные данные могут обрабатываться оператором **только при наличии письменного согласия субъекта** персональных данных (за исключением случаев, установленных в ч. 2 ст. 11 Закона) (ч. 1 ст. 11 Закона).

Исключения:

- в связи с осуществлением правосудия и исполнением судебных актов,
- в связи с проведением обязательной государственной дактилоскопической регистрации,
- а также в случаях, предусмотренных зак-вом РФ об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе.

Обращаем внимание на уникальный материал в КонсультантПлюс:



Персональные данные субъекта, разрешенные им для распространения – как отдельная категория.

В марте 2021 года из законодательства исчезло понятие «общедоступные данные» и оно было заменено на вот эти «персональные данные, разрешенные для распространения».

Согласно ныне действующему законодательству, возможно распространять персональные данные в случае, если имеется согласие субъекта персональных данных (ст. 10.1 Закона N 152-ФЗ). На практике это означает, что, например, перед публикацией сведений в интернете пользователь должен дать согласие на то, что его сведения будут опубликованы, и это согласие является достаточно сложным и детальным документом.

Такой подход в работе с ПД реализуется при размещении информации на общедоступных ресурсах с неограниченным доступом третьих лиц.

Мы видим субъекта персональных данных и видим некий интернет-сайт – общедоступный источник информации. Субъект – это пользователь, который, например, хочет разместить свое резюме на сайте по поиску работы. У сайта есть владелец, и этот владелец, согласно новой редакции закона, должен запросить согласие у субъекта персональных данных.

Причем согласие составляется в соответствии с требованиями, установленными в **Приказе Роскомнадзора от 21.06.2021 N 106**.

Это согласие является достаточно детальным документом, и его можно получить, либо используя веб-форму на сайте, либо используя единую систему идентификации и аутентификации.

Только после того, как субъект персональных данных выразит свое согласие на размещение данных на сайте, их можно будет опубликовать. Согласие содержит очень много информации. В том числе там даже указывается та информация, которая может быть не нужна самому сайту, которую не планируется на этом сайте публиковать.

Сам **образец согласия на обработку ПД** утвержден Приказом Роскомнадзора от 24.02.2021 N 18 «Об утверждении требований к содержанию согласия …».

СОГЛАСИЕ на обработку персональных данных.

Закон требует, чтобы ПД обрабатывались оператором при наличии СОГЛАСИЯ.

Приведем несколько примеров, когда законодательство предписывает обязательно получить согласие на обработку персональных данных. Их можно найти в **ст. 10, 11 Закона** N 152-ФЗ (они касаются обработки биометрических данных и специальных категорий персональных данных).

В **ст. 10.1 Закона N 152-ФЗ** говорится о необходимости получить согласие для распространения персональных данных, причем это согласие должно соответствовать требованиям, установленным Приказом Роскомнадзора от 24.02.2021 N 18.

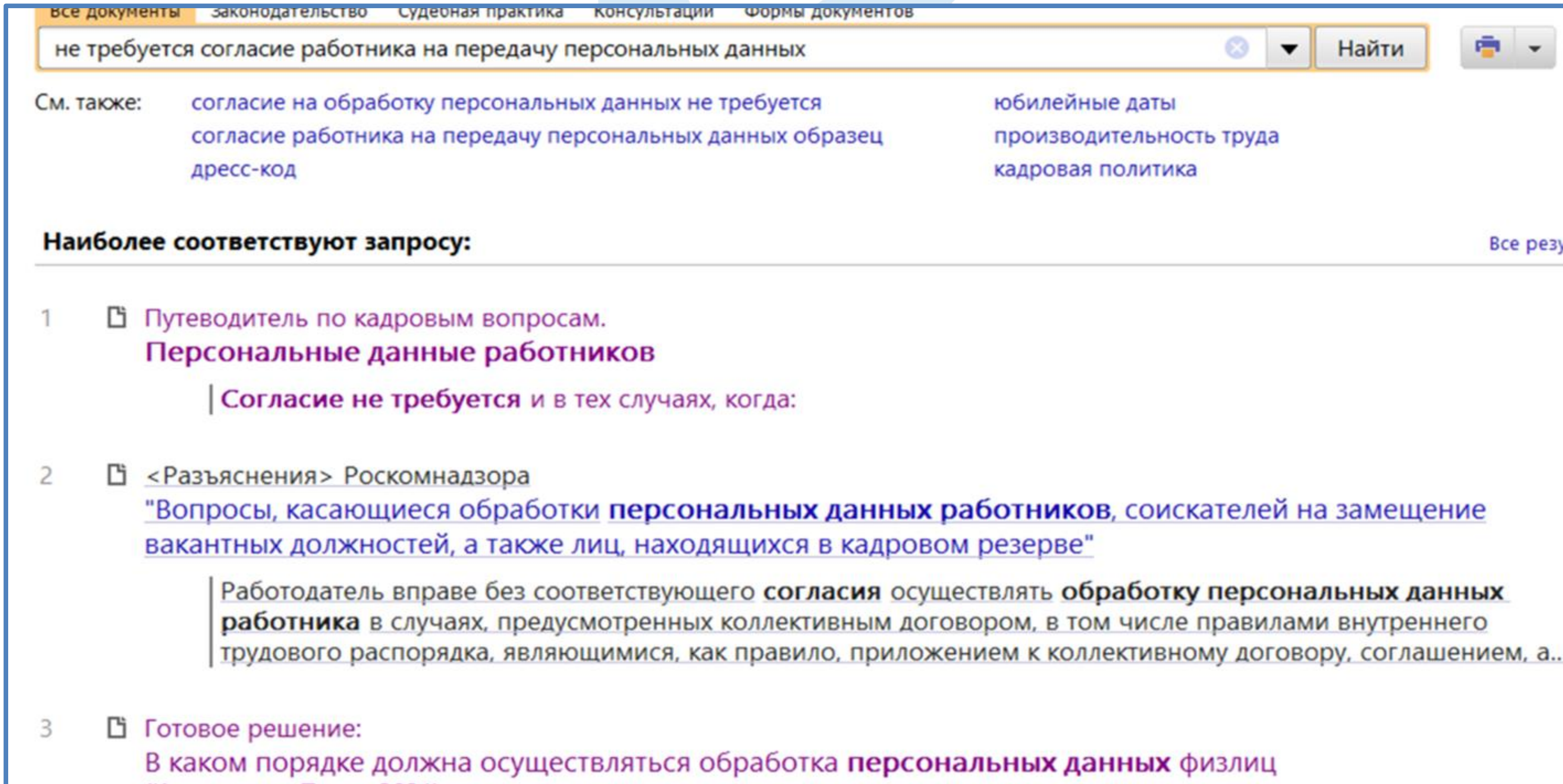
В **ст. 12 Закона N 152-ФЗ** говорится о необходимости получения согласия на обработку ПД при передаче их в страны, не обеспечивающие адекватного уровня защиты прав субъектов персональных данных (ч. 4 ст. 12 Закона N 152-ФЗ).

В **ст. 15 Закона N 152-ФЗ** идет речь о согласии на обработку ПД в тех случаях, когда оператор осуществляет прямые контакты с гражданами для продвижения им товаров, а также в рамках политической агитации.

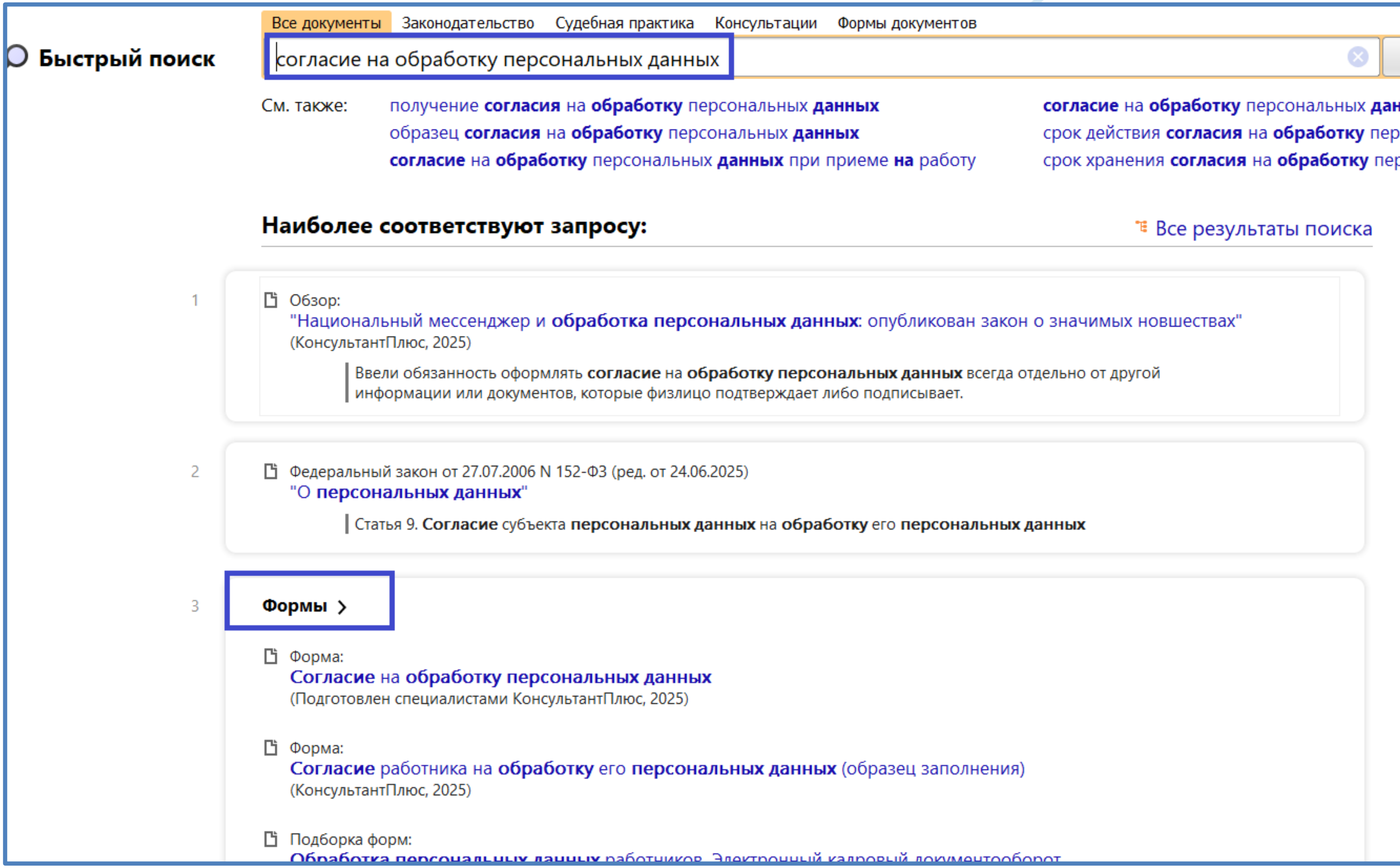
В **ст. 88 ТК РФ** указано, когда необходимо получить согласие работника, являющегося субъектом ПД. Например, при передаче его данных третьим лицам или при использовании его данных в коммерческих целях организации-работодателя .

Обращаем внимание – согласие может не требоваться:

В случаях, исчерпывающий перечень которых содержится в **п.2 ч. 1 ст. 6 Закона о персональных данных**, согласие субъекта ПД не требуется, обработка их осуществляется на основании закона.



Образцы согласий можно получить в К+



Обращаем внимание, что с 1 сентября 2025 года **согласие на обработку ПД всегда должно быть оформлено отдельным документом** - в силу вступают поправки к ст. 9 закона № 152-ФЗ «О персональных данных», которые обязывают это делать.

Раньше компании и предприниматели часто включали формулировки о согласии в тексты других бумаг (договоров, анкет, заявлений), либо объединяли несколько разных согласий в один документ. С 1 сентября 2025 года такой подход строго запрещен — за нарушение грозят серьезные штрафы. **Согласие должно предоставляться как самостоятельный документ, отдельно от иных сведений и документов, которые подписывает субъект персональных данных.**

Запрещено не только «прятать» согласие внутри других бумаг, но и объединять разные виды согласий в одном документе.

Раньше компании зачастую комбинировали:

- ✓ согласие на обработку персональных данных;
- ✓ согласие на рекламную рассылку;
- ✓ согласие на распространение данных.

С 1 сентября 2025 года так делать нельзя — каждый вид согласия оформляется отдельно.

Изменения касаются только тех согласий, которые оформляются после 1 сентября 2025 года. Все ранее полученные согласия продолжают действовать, их переподписывать не требуется.

Штрафы за отсутствие отдельного согласия.

После 1 сентября 2025 года согласие, полученное «в составе» другого документа, будет считаться недействительным. Обработка данных без законного согласия - правонарушение. Штрафы по ст. 13.11 КоАП:

- ✓ для граждан — от 10 000 до 15 000 рублей;
- ✓ для должностных лиц — от 100 000 до 300 000 рублей;
- ✓ для юридических лиц и ИП — от 300 000 до 700 000 рублей.

При повторном нарушении:

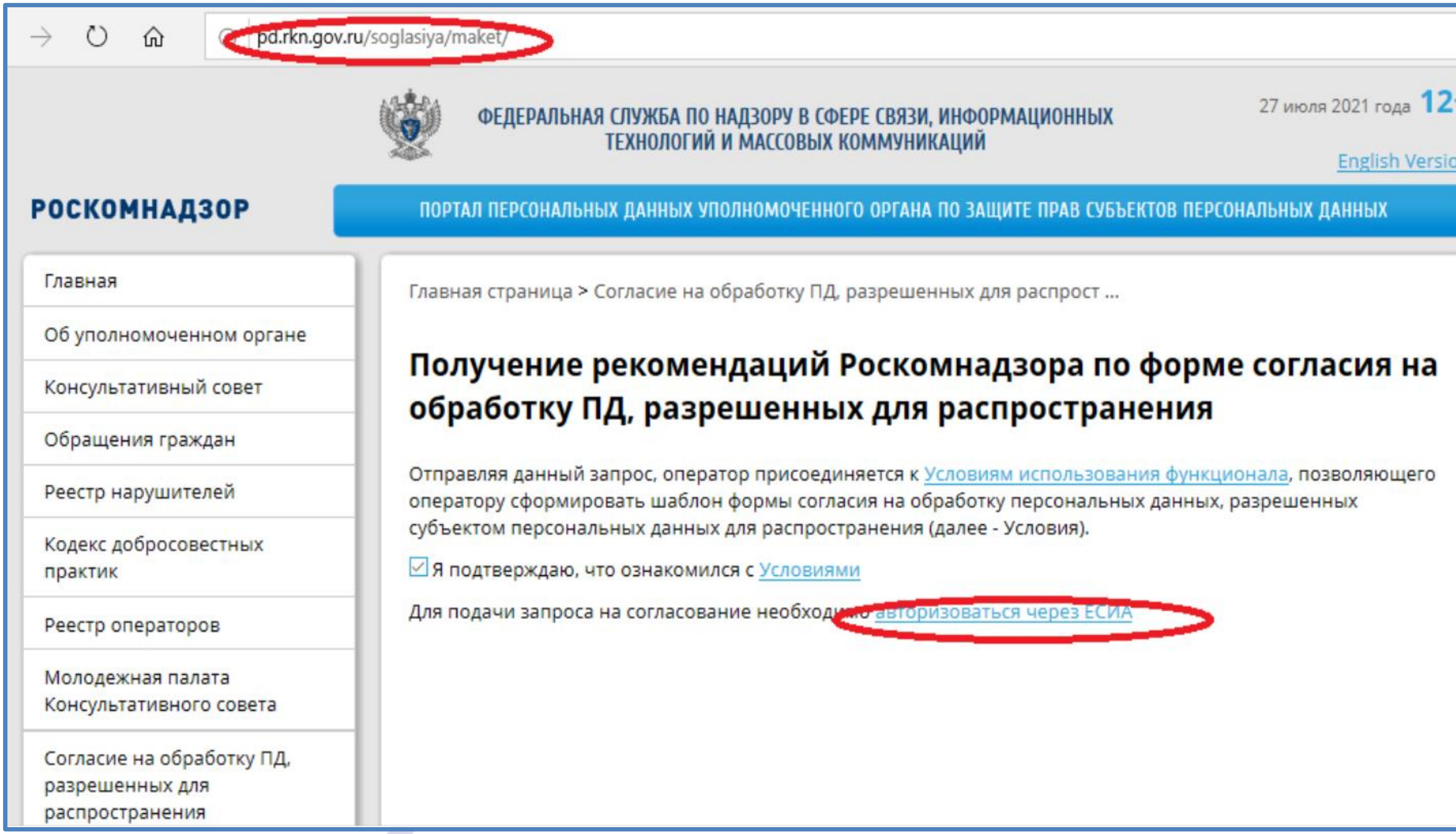
- ✓ граждане — до 30 000 рублей,
- ✓ должностные лица — до 500 000 рублей,
- ✓ ИП — от 500 000 до 1 000 000 рублей,
- ✓ компании — до 1 500 000 рублей.

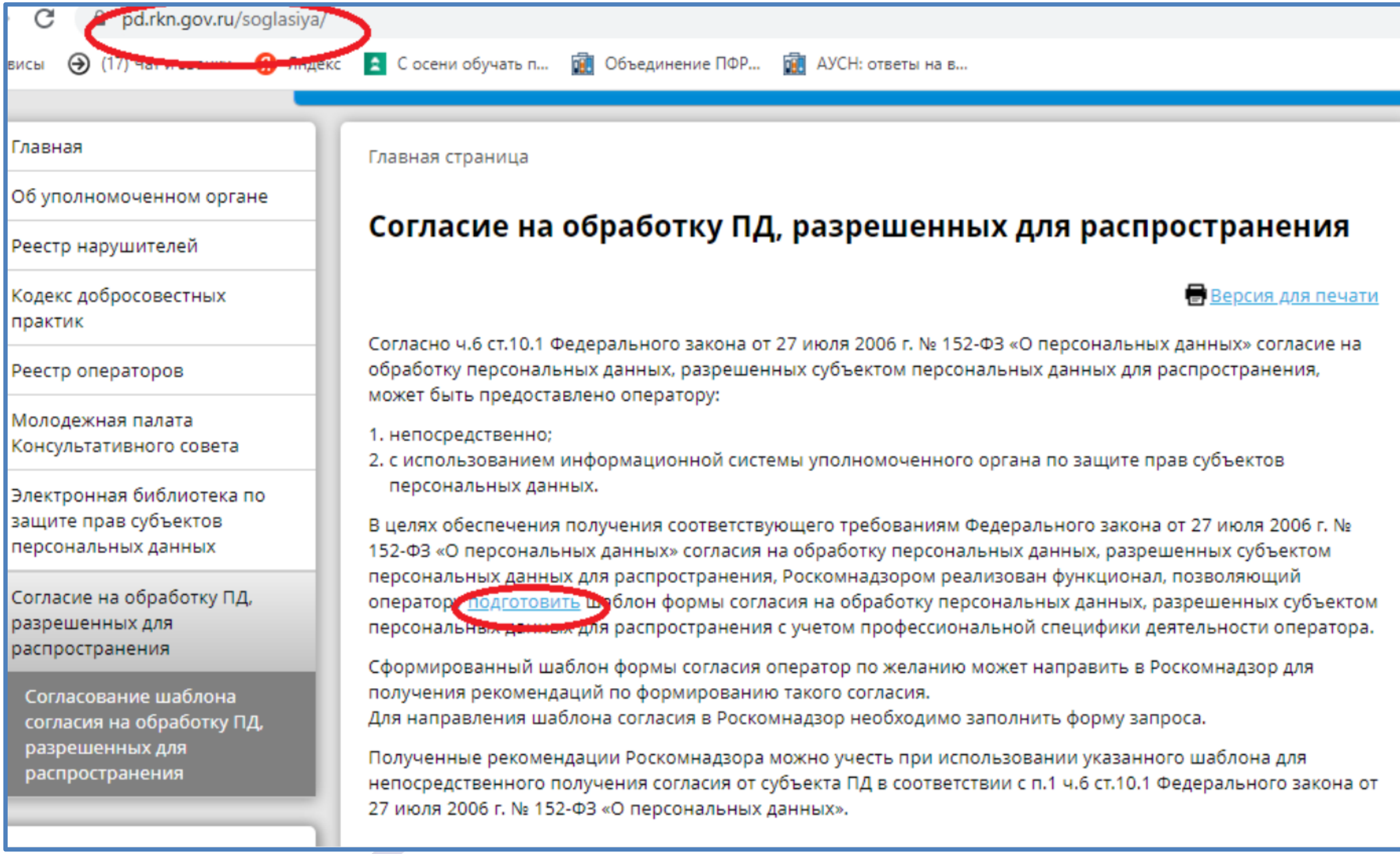
Роскомнадзор предлагает сервис для подготовки формы согласия на обработку персональных данных.

С 1 июля 2021 года заработал новый интернет-сервис для операторов персональных данных. Он поможет правильно подготовить шаблон формы согласия на обработку данных, которые лицо разрешило распространять. В нем уже учтены обязательные требования.

Оператор заполнит необходимые поля в формате конструктора. Шаблон рассмотрит специалист Роскомнадзора и при необходимости даст рекомендации по доработке. Форму согласия оператор сможет использовать в своей деятельности.

Информация Роскомнадзора от 01.07.2021.


pd.rkn.gov.ru/soglasiya/maket/
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ
27 июля 2021 года
English Version
РОСКОМНАДЗОР
ПОРТАЛ ПЕРСОНАЛЬНЫХ ДАННЫХ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ
Главная
Об уполномоченном органе
Консультативный совет
Обращения граждан
Реестр нарушителей
Кодекс добросовестных практик
Реестр операторов
Молодежная палата Консультативного совета
Согласие на обработку ПД, разрешенных для распространения
Главная страница > Согласие на обработку ПД, разрешенных для распрост ...
Получение рекомендаций Роскомнадзора по форме согласия на обработку ПД, разрешенных для распространения
Отправляя данный запрос, оператор присоединяется к Условиям использования функционала, позволяющего оператору сформировать шаблон формы согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения (далее - Условия).
Я подтверждаю, что ознакомился с Условиями
Для подачи запроса на согласование необходимо авторизоваться через ЕСИА



pd.rkn.gov.ru/soglasiya/

Главная

Об уполномоченном органе

Реестр нарушителей

Кодекс добросовестных практик

Реестр операторов

Молодежная палата Консультативного совета

Электронная библиотека по защите прав субъектов персональных данных

Согласие на обработку ПД, разрешенных для распространения

Согласование шаблона согласия на обработку ПД, разрешенных для распространения

Главная страница

Согласие на обработку ПД, разрешенных для распространения

Версия для печати

Согласно ч.6 ст.10.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:

1. непосредственно;
2. с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

В целях обеспечения получения соответствующего требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, Роскомнадзором реализован функционал, позволяющий оператору подготовить шаблон формы согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения с учетом профессиональной специфики деятельности оператора.

Сформированный шаблон формы согласия оператор по желанию может направить в Роскомнадзор для получения рекомендаций по формированию такого согласия.
Для направления шаблона согласия в Роскомнадзор необходимо заполнить форму запроса.

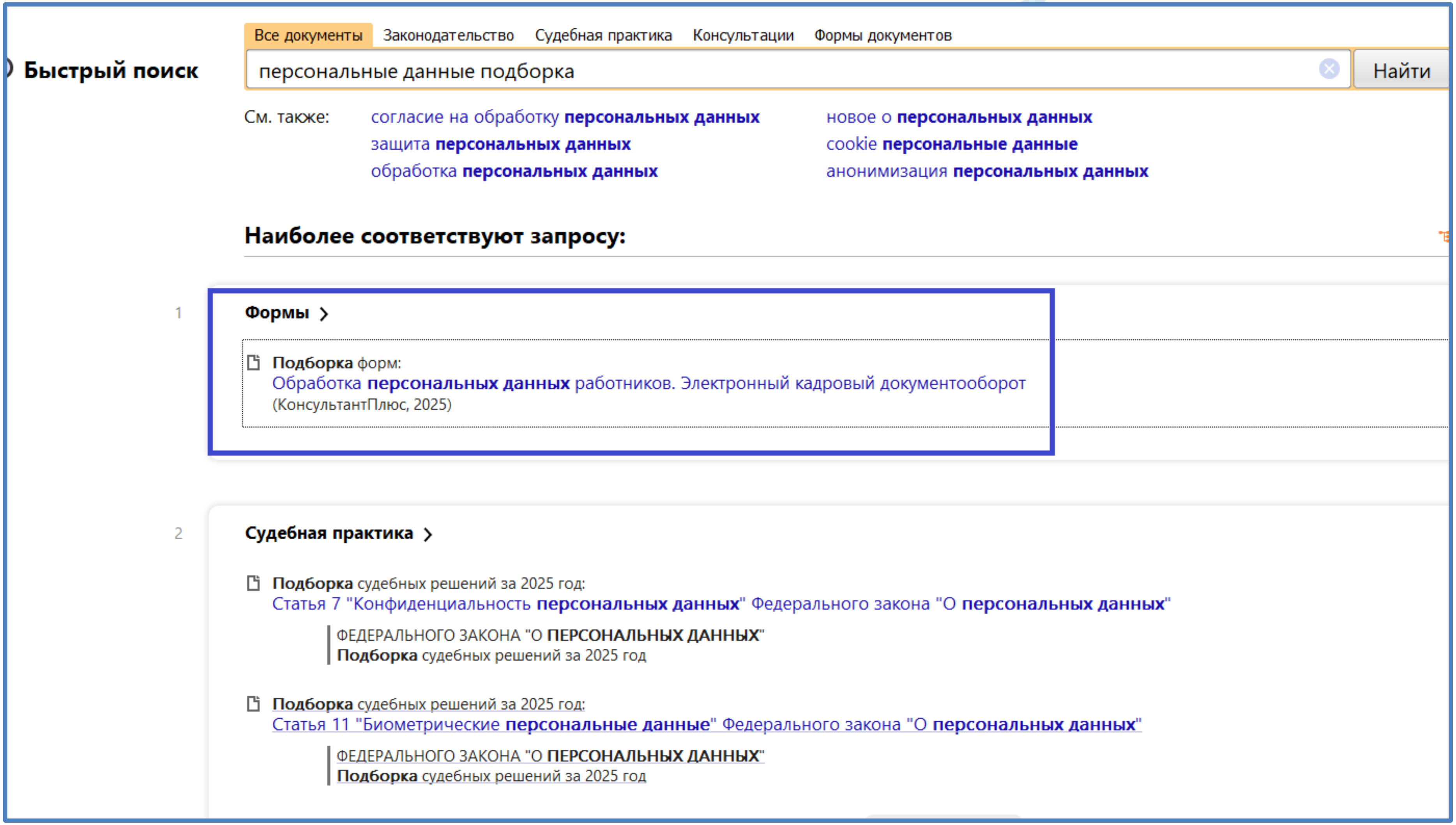
Полученные рекомендации Роскомнадзора можно учесть при использовании указанного шаблона для непосредственного получения согласия от субъекта ПД в соответствии с п.1 ч.6 ст.10.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Когда нужно получать согласие работника на распространение персональных данных?

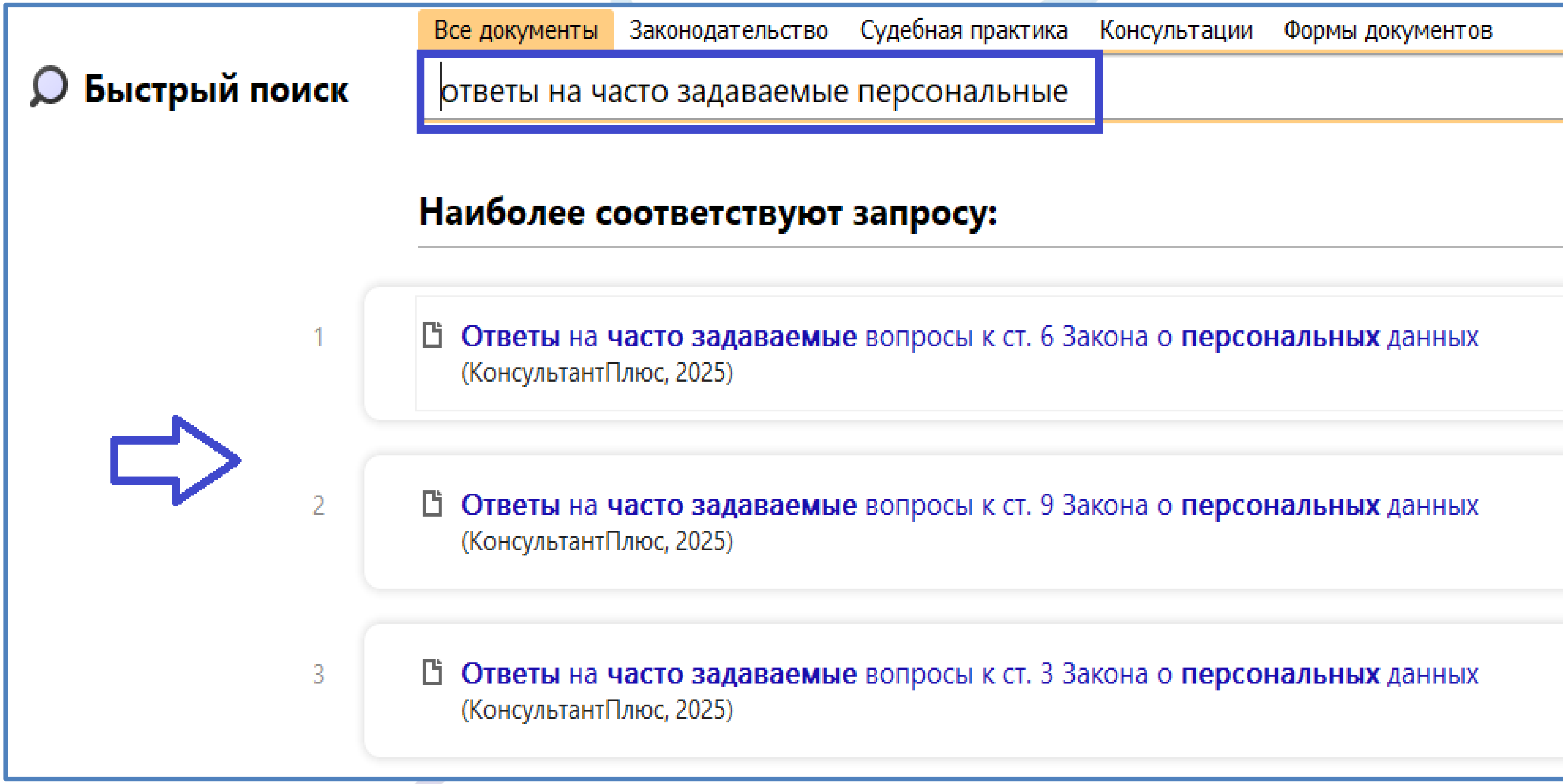
Заверенное разрешение нужно получать с человека каждый раз, когда планируется передача личной информации, а также его публикация.

- ✓ размещение сведений о работнике на официальном сайте компании;
- ✓ размещение фото, ФИО и прочих сведений на доске почета;
- ✓ размещение заметок в бумажных и электронных СМИ;
- ✓ передача данных работника охранной компании для выписка пропуска на территорию организации;
- ✓ прочие случаи распространения информации в различных целях.

Поиск важной информации в КонсультантПлюс – Подборка форм со всеми шаблонами.



Поиск важной информации в КонсультантПлюс – уникальные материалы «Ответы на часто задаваемые вопросы». Готовые решения в одной подборке.



Как действовать при приеме нового работника - подсказки кадровику.

- ✓ При приеме оформляйте стандартное согласие.
- ✓ Если планируете публикацию сведений, берите второе разрешение — на распространение сведений.
- ✓ Из стандартного согласия на обработку нужно исключить слова «распространение» и «передача» Оформлять, как раньше, согласие на передачу в свободной форме теперь запрещено

Путеводитель по кадровым вопросам. Персональные данные работников

Когда и как нужно получать согласие работника на обработку персональных данных

Обработка персональных данных осуществляется с согласия работника. Оно должно быть конкретным, предметным, информированным, сознательным, однозначным. Согласие оформляется отдельно от иных информации и (или) документов, которые подтверждает и (или) подписывает работник (п. 1 ч. 1 ст. 6, ч. 1 ст. 9 Закона о персональных данных).

Поскольку в случае возникновения спора доказать получение согласия работника на обработку его персональных данных должен работодатель (ч. 3 ст. 9 Закона о персональных данных), целесообразно оформить такое согласие письменно. В некоторых случаях письменная форма согласия прямо предусмотрена законом (ч. 4 ст. 9 Закона о персональных данных). Например, письменное согласие работника на обработку его персональных данных требуется:

- при получении персональных данных работника у третьей стороны (п. 3 ст. 86 ТК РФ). Подробнее об этом см. п. 2 настоящего материала;

- при передаче персональных данных работника третьим лицам, кроме тех случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, а также в иных предусмотренных федеральными законами случаях (абз. 2 ст. 88 ТК РФ);

Обязанности в случае компрометации персональных данных.

Не забудьте, что у компании есть 24 часа с момента происшествия, чтобы сообщить в Роскомнадзор:

- ✓ об инциденте;
- ✓ его предполагаемой причине и вреде, причиненном субъектам данных;
- ✓ мерах по устранению последствий инцидента;
- ✓ представителе компании, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с происшествием.

У компании есть 72 часа с момента инцидента, чтобы провести внутреннее расследование и сообщить в Роскомнадзор о его результатах. На сайте Роскомнадзора доступны специальные электронные формы подачи уведомлений (https://pd.rkn.gov.ru/incidents/form/).

ГосСОПКА.

С 1 сентября 2022 года появилась обязанность оператора обеспечивать взаимодействие с ГосСОПКА - системой обнаружения, предупреждения, ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

По закону (в его новых требованиях) взаимодействовать с этой системой должны все операторы персональных данных. При этом интеграция с ГосСОПКА **не подразумевает обязательное подключение к системе в физическом плане**. В ряде случаев достаточно организовать канал передачи информации (например, через электронную почту, по которой будут сообщены все данные, если произошли события, указанные в 152-ФЗ).

На оператора ПД теперь возложена обязанность обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ - ГосСОПКА (см. ст. 5 Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»), включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных (ч. 12 ст. 19 Закона N 152-ФЗ).

Такая мера позволяет повысить гарантии информационной безопасности нашей страны в целом за счет эффективной и слаженной защиты всех ее информационных элементов на самых различных уровнях.

ГосСОПКА.

Взаимодействие с системой для ИП и юрлиц означает передачу информации о компьютерных инцидентах на своих сетях:

- ✓ даты, времени, места происшествия;
- ✓ наличие связи между инцидентом и компьютерной атакой;
- ✓ технические параметры компьютерного инцидента;
- ✓ последствия.

Операторы, которые технически не подключены к ГосСОПКА, направляют информацию по E-mail, телефону, факсу на контакты НКЦКИ, указанные на сайте **http://cert.gov.ru**.

Дополнительно (кроме взаимодействия с ГосСОПКА) оператор обязан сообщать в Роскомнадзор об утечках персональных данных (ч. 3.1 ст. 21 152-ФЗ). В течение 24 часов после происшествия он информирует об инциденте, предполагаемом вреде субъекту ПД, а также о должностном лице, уполномоченном на взаимодействие с Роскомнадзором по данному инциденту. Через 72 часа оператор сообщает о результатах расследования утечки данных. Это делают те же лица. Указанные в локальном акте по вопросу защиты ПД.

Взаимодействие с Роскомнадзором осуществляется через портал Госуслуг. Оператору нужна подтвержденная учетная запись на Госуслугах, привязанная к личному кабинету организации.

Защита персональных данных при их обработке: рекомендации Роскомнадзора операторам.

Ведомство советует операторам:

- ✓ минимизировать список ПД для сбора и обработки, использовать только те сведения, которые реально нужны;
- ✓ раздельно хранить личные сведения клиентов, работников, соискателей и т.д.;
- ✓ не накапливать личную информацию на всякий случай и не формировать профили клиентов;
- ✓ хранить идентификаторы человека (Ф.И.О., электронную почту, телефон, адрес) и данные о взаимодействии с ним (информацию об оказании услуг и продаже товаров, переписку, договоры и пр.) в базах данных, которые напрямую не связаны друг с другом.

РАБОТА в системе КОНСУЛЬТАНТ ПЛЮС

Все документы Законодательство Судебная практика Консультации Формы документов

Быстрый поиск защита персональных данных

См. также: **защита персональных данных** оператором
защита персональных данных работников
положение о **персональных данных**
требования к **защите персональных данных**
косгу **защита персональных данных**
приказ о **защите персональных данных** работников

Наиболее соответствуют запросу: Все результаты поиска

3 Готовое решение:
Какие меры по **защите персональных данных** физлиц нужно принимать при обработке этих **данных**
(КонсультантПлюс, 2025)

4 "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ
(ред. от 29.09.2025)
Глава 14. **Защита персональных данных** работника

5 Готовое решение:
Какие меры по **защите персональных данных** работников должны приниматься при обработке этих **данных**
(КонсультантПлюс, 2025)

6 Типовая ситуация:
Обработка **персональных данных** работников: требования, документы, штрафы
(Издательство "Главная книга", 2025)
В положении о **защите персональных данных** работников установите порядок работы с **данными**, перечень лиц, имеющих к ним доступ, правила хранения личных дел и других кадровых документов, способы **защиты** электронных документов. Утвердите положение приказом руководителя и ознакомьте с ним работников под роспись (ст. 88 ТК РФ...

Проверки Роскомнадзора.

Обновлен порядок осуществления федерального государственного контроля (надзора) за обработкой персональных данных - **Постановление Правительства РФ от 29.06.2021 N 1046.**

При осуществлении федерального государственного контроля (надзора) применяется система оценки и управления рисками – риск-ориентированный подход.

Поднадзорные объекты относятся к одной из следующих категорий риска причинения вреда (ущерба): **высокий риск, значительный риск, средний риск, умеренный риск и низкий риск**. Установлены критерии отнесения объектов к категориям риска.

При осуществлении государственного контроля (надзора) за обработкой персональных данных могут проводиться такие виды профилактических мероприятий, как **информирование, обобщение правоприменительной практики, объявление предостережения, консультирование и профилактический визит.**

К контрольным (надзорным) мероприятиям относятся: **инспекционный визит, документарная проверка и выездная проверка.**

Установлена периодичность таких мероприятий.

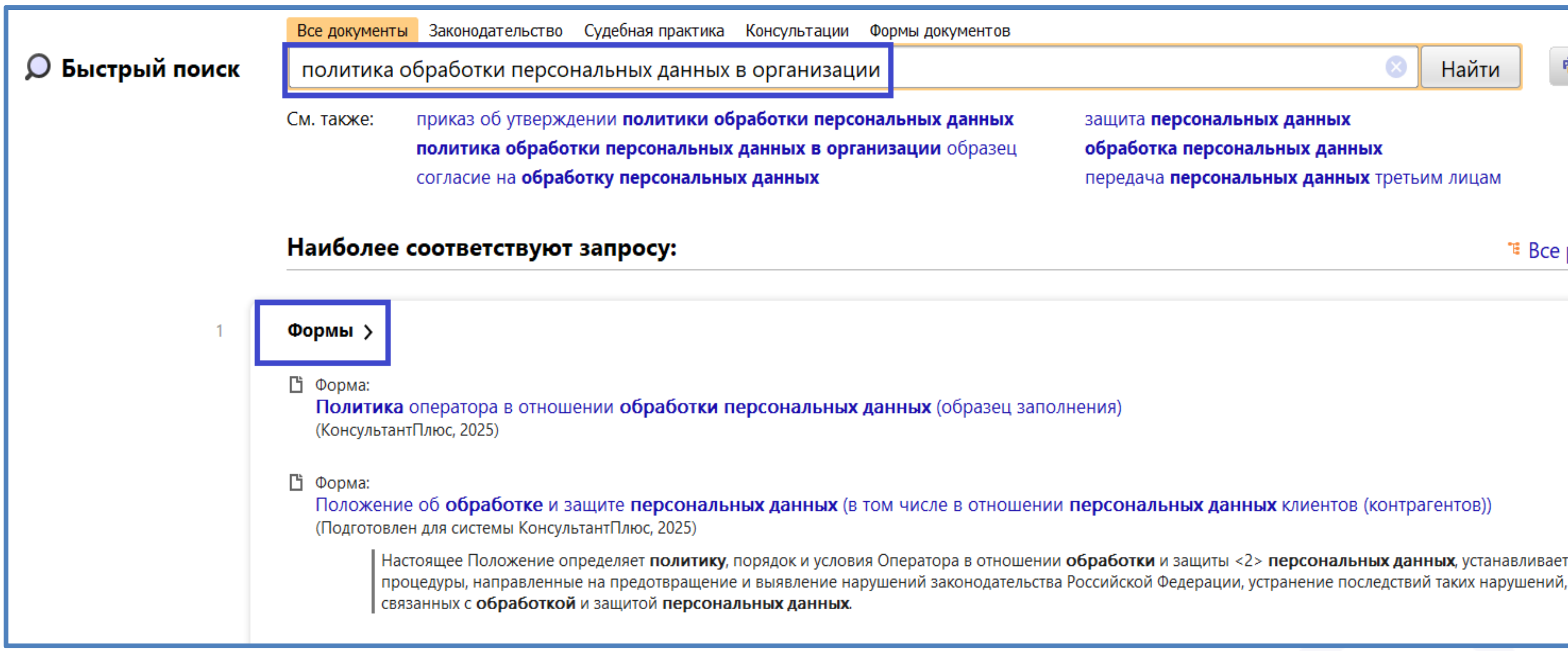
Роскомнадзор дал разъяснения, касающиеся документа, определяющего политику оператора в отношении обработки персональных данных.

Указано, в частности, следующее:

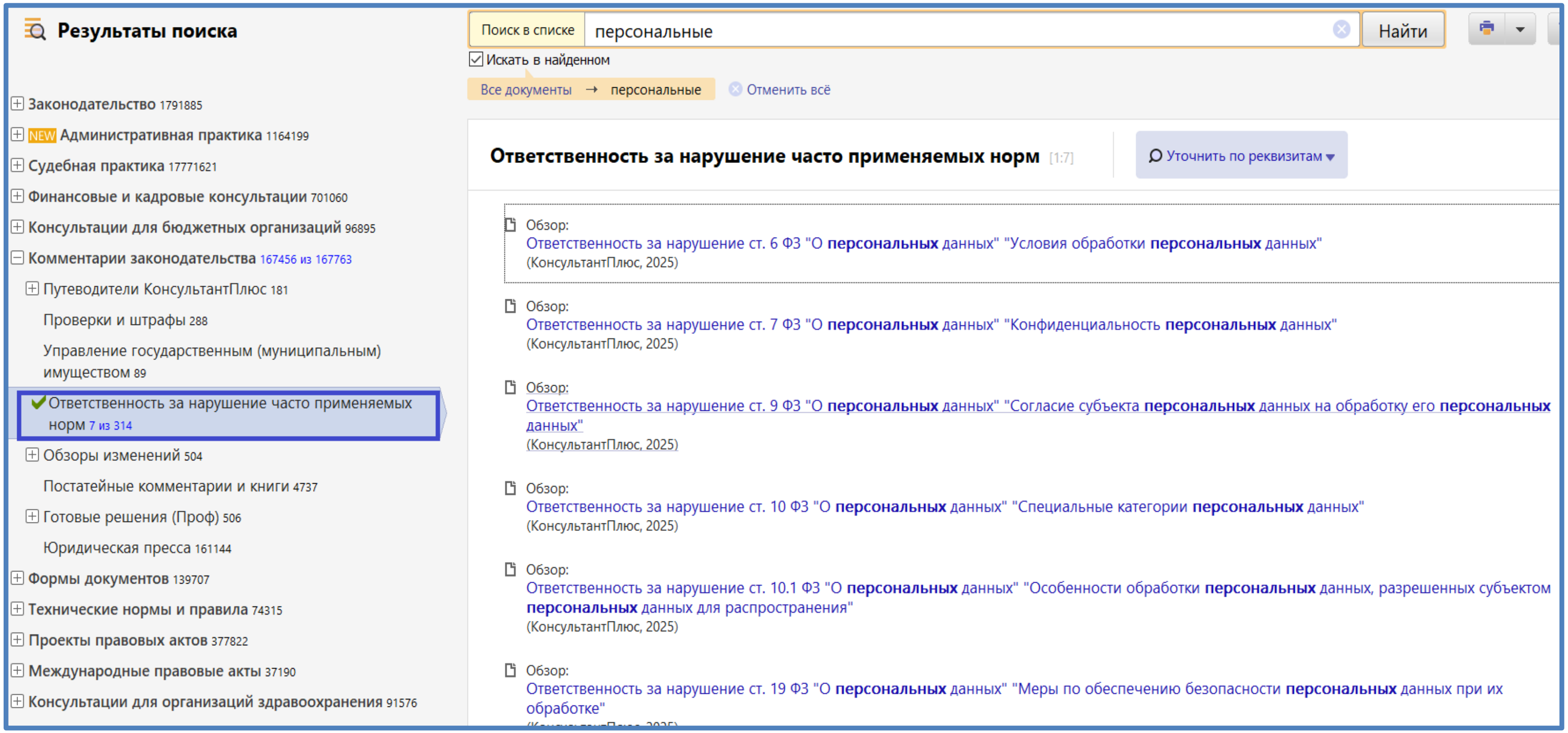
- ✓ все операторы независимо от способа сбора персональных данных должны иметь указанный документ и обеспечить неограниченный доступ к нему;
- ✓ предоставить возможность доступа к указанному документу с использованием средств информационно-телекоммуникационных сетей обязаны только операторы, осуществляющие сбор персональных данных с использованием таких сетей;

- ✓ определять структуру и содержание политики обработки персональных данных должен оператор.

Письмо Роскомнадзора от 19.10.2021 N 08-71063.



РАБОТА в системе КОНСУЛЬТАНТ ПЛЮС



КОМПАС ЛИДЕРА

УВЕДОМЛЕНИЕ РОСКОМНАДЗОРА.

Обращаем внимание на изменения для тех, кто является ОПЕРАТОРАМИ по обработке ПД!

Еще с 1 сентября 2022 года вступили в силу изменения в закон «О персональных данных».

Теперь операторы должны уведомлять Роскомнадзор о начале или осуществлении **любой обработки персональных данных** за исключением случаев, когда данные обрабатываются в целях защиты безопасности государства и общественного порядка, транспортной безопасности, или если оператор обрабатывает данные исключительно без средств автоматизации.

Электронные формы см. по адресу https://pd.rkn.gov.ru/operators-registry/notification/

Ведомство также утвердило формы уведомлений:

- ✓ об изменении сведений в уведомлении о намерении обрабатывать персональные данные;
- ✓ прекращении обработки персональных данных.

Приказ Роскомнадзора от 28.10.2022 N 180

На портале Роскомнадзора оператору предоставлена возможность сформировать и отправить уведомление в территориальный орган Роскомнадзора одним из следующих способов:

- ✓ в бумажном виде;
- ✓ в электронном виде с использованием усиленной квалифицированной электронной подписи.

Оператор обязан уведомить Роскомнадзор о своем намерении осуществлять обработку персональных данных (за исключением отдельных случаев) (ч. 1 ст. 22 Закона о персональных данных).

Уведомление о намерении осуществлять обработку персональных данных нужно подать в Роскомнадзор до начала их обработки (ч. 1 ст. 22 Закона о персональных данных).

Уведомление о начале обработки персональных данных работников должен подавать работодатель. Это обусловлено тем, что именно он в данном случае признается оператором (п. 2 ст. 3, ч. 1 ст. 22 Закона о персональных данных).

Составьте уведомление по форме, приведенной в Приложении N 1 к Приказу Роскомнадзора от 28.10.2022 N 180.

В уведомлении укажите, в частности (ч. 3, 3.1 ст. 22 Закона о персональных данных):

- ✓ свое наименование (фамилию, имя, отчество), адрес;
- ✓ цель обработки персональных данных. Для каждой цели необходимо указать ряд сведений, в частности: категории персональных данных, категории субъектов, способы обработки персональных данных, правовое основание обработки персональных данных;
- ✓ описание мер, предусмотренных ст. ст. 18.1 и 19 Закона о персональных данных. Что указывать в качестве описания мер, предусмотренных ст. ст. 18.1 и 19 Закона о персональных данных, при заполнении уведомления об обработке персональных данных смотрите в Готовом решении: **Каковы обязанности оператора персональных данных** (КонсультантПлюс, 2025).

- ✓ дату начала обработки персональных данных. В качестве даты начала обработки персональных данных при заполнении уведомления рекомендуем указывать ту дату, в которую оператор планирует фактически приступить к обработке персональных данных.
- ✓ срок или условие прекращения обработки персональных данных;
- ✓ сведения об обеспечении безопасности персональных данных в соответствии с установленными требованиями к защите таких данных.

Уведомление должно быть подписано уполномоченным лицом (ч. 3 ст. 22 Закона о персональных данных).

Роскомнадзор на основании этого уведомления в течение 30 дней с даты его поступления должен внести сведения в реестр операторов (ч. 4 ст. 22 Закона о персональных данных).

Если сведения, содержавшиеся в ранее поданном уведомлении, изменились, то нужно уведомить Роскомнадзор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли изменения, обо всех произошедших за указанный период изменениях.

Если вы прекратили обработку персональных данных, нужно уведомить Роскомнадзор в течение 10 рабочих дней с даты прекращения обработки персональных данных (ч. 7 ст. 22 Закона о персональных данных).

Путеводитель по госуслугам для юридических лиц. Представление уведомления об обработке персональных данных

↑ ПУТЕВОДИТЕЛЬ ПО ГОСУСЛУГАМ ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ ПРЕДСТАВЛЕНИЕ УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬН...

ПРЕДСТАВЛЕНИЕ УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Все формы уведомлений ищите в КонсультантПлюс:

Все документы Законодательство Судебная практика Консультации **Формы документов**

Быстрый поиск уведомление роскомнадзора об обработке персональных данных Найти

См. также: образец **уведомления об обработке персональных данных**
форма **уведомления об обработке персональных данных**
порядок предоставления **уведомлений об обработке персональных данных** ...
обработка персональных данных без уве
цель **обработки персональных данных** в
уведомление о прекращении **обработки**

Формы документов. Наиболее соответствуют запросу: Вс

1 Форма:
Уведомление о намерении осуществлять **обработку персональных данных** работников (образец заполнения)
(КонсультантПлюс, 2025)

2 Форма:
Уведомление о намерении **обрабатывать персональные данные** (образец заполнения)
(КонсультантПлюс, 2025)

3 Форма:
Уведомление о прекращении **обработки персональных данных**
(Приказ **Роскомнадзора** от 28.10.2022 N 180)

4 Форма:
Уведомление о намерении осуществлять **обработку персональных данных**
(Приказ **Роскомнадзора** от 28.10.2022 N 180)

Утечка персональных данных и другие нарушения операторов: изменения 2025 года.

С 30 мая 2025 года операторам персональных данных грозят крупные штрафы по КоАП РФ за действия (бездействие), из-за которых произошла незаконная передача этих сведений. Начали применяться более строгие наказания за непредставление Роскомнадзору ряда уведомлений.

Утечка персональных данных.

В случае незаконной передачи информации о людях в количестве от 1 тыс. до 10 тыс. человек грозит штраф:

- ✓ должностным лицам государственного или муниципального органа либо некоммерческой организации - от 200 тыс. до 400 тыс. руб.;

- ✓ ИП и компаниям - от 3 млн до 5 млн руб.

На те же суммы оштрафуют в случае утечки от 10 тыс. до 100 тыс. идентификаторов физлиц. Это уникальные обозначения, которые находятся в информсистемах операторов.

За более масштабные происшествия ввели более крупные штрафы.

Неправомерное распространение персональных данных спецкатегорий обернется штрафом:

- ✓ для упомянутых должностных лиц - от 1 млн до 1,3 млн руб.;
- ✓ для ИП и компаний - от 10 млн до 15 млн руб.

Ранее таких составов в КоАП РФ не было.

Неуведомление Роскомнадзора

За несообщение ведомству об утечке, которой нарушены права субъектов персональных данных, назначат такие штрафы:

- ✓ должностным лицам государственного или муниципального органа либо некоммерческой организации - от 400 тыс. до 800 тыс. руб.;
- ✓ ИП и компаниям - от 1 млн до 3 млн руб.

За неуведомление о намерении обрабатывать личную информацию грозит штраф:

- ✓ упомянутым должностным лицам - от 30 тыс. до 50 тыс. руб.;
- ✓ ИП и компаниям - от 100 тыс. до 300 тыс. руб.

Такие же наказания установили для тех, кто известил Роскомнадзор несвоевременно.

Нарушение прав потребителей.

Отказ заключить, исполнить, изменить или расторгнуть договор с потребителем из-за того, что он не стал проходить идентификацию (аутентификацию) по биометрии, повлечет штраф:

- ✓ для любых должностных лиц и ИП - от 50 тыс. до 100 тыс. руб.;
- ✓ для любых компаний - от 200 тыс. до 500 тыс. руб.

Этот состав станет исключением из действующего правила. По нему штрафуют за отказ потребителю из-за того, что он правомерно не предоставил персональные сведения. Размер санкций по данному правилу в несколько раз ниже.

Федеральный закон от 30.11.2024 N 420-ФЗ.

Обезличивание ПД – требования с 1 сентября 2025 года.

С 1 сентября 2025 года надо направлять по запросу Минцифры обезличенные персональные данные. Цель изменений — дать бизнесу и государству возможность использовать большие данные для аналитики, развития искусственного интеллекта, технологий, статистики без нарушения конфиденциальности и прав личности.

Главные изменения:

- ✓ Обязательное предоставление по требованию Минцифры обезличенных сведений в Единую информационную платформу национальной системы управления данными (ЕИП НСУД).

- ✓ Возможность обрабатывать обезличенные ПДн без согласия клиента. Ранее согласие требовалось в большинстве случаев обработки ПДн.
- ✓ Обезличивание ПДн становится более выгодной альтернативой уничтожению ПДн. Этими данными можно пользоваться для аналитических, маркетинговых и иных целей бизнеса.

Информация обезличивается таким образом, чтобы связь с личностью конкретного человека была разорвана, но содержательность информации для последующей обработки сохранилась: можно будет подсчитать количество клиентов из конкретного города, возрастной группы, способ доставки товара, сумму заказа, предпочтения клиента и другое для целей аналитики.

Обезличивание — изменение данных о субъекте таким образом, что без дополнительной расшифровки нельзя понять, какому именно человеку они принадлежат. Это способ защиты ПД от несанкционированного доступа злоумышленников.

Запрещено обезличивать ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни (ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», далее — Закон № 152-ФЗ). Исключением является обработка этих ПДн в социально-значимых процессах: перепись населения, правосудие, статистика медицинских организаций и т.п.

Обезличивание ПД проводят специальными методами, разбираться в которых — компетенция специалистов по информационной безопасности. Но кадровику и бухгалтеру тоже полезно знать основы этой процедуры, потому что в кадрах и бухгалтерии хранится большое количество личной информации работников, сотрудников подрядчика. И эти службы отвечают за безопасность ПД. Кроме того, именно кадровик и бухгалтер определяют, данные каких категорий субъектов будут шифроваться.

Причины для обезличивания установлены законом. Так, при достижении целей обработки оператор обязан обезличить или уничтожить ПД субъекта (ч. 7 ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ). **Это правило действовало и до 1 сентября 2025 года.**

Теперь появился случай, когда оператор должен обезличить ПД по закону — требование Минцифры (ч. 2 ст. 13.1 Федерального закона от 27.07.2006 № 152-ФЗ — действует с 1 сентября 2025 года). Вышел **Приказ Роскомнадзора от 19.06.2025 № 140**. Он содержит требования к обезличиванию и методы обезличивания для большинства случаев обработки ПД.

Главное нововведение — обезличенные ПД с 1 сентября 2025 года можно обрабатывать без получения согласия гражданина. Ранее оно требовалось обязательно, но теперь чётко разрешено использовать обезличенные данные без согласия субъекта для исследований или технологий без нарушения закона. Важно: обезличивание должно исключать возможность прямой идентификации гражданина по этим данным.

Существенное изменение — **теперь операторов ПД могут обязать предоставлять обезличенные сведения в государственную информационную систему (ГИС). Минцифры получило право направлять компаниям и ведомствам требования предоставить нужные данные в обезличенном виде для загрузки в федеральную ГИС.** Правительство РФ определило, что такой системой станет Единая информационная платформа нацсистемы управления данными (ЕИП НСУД) с новой подсистемой обезличенных данных.

Проще говоря, если государству понадобятся большие массивы данных для аналитики или социальных проектов, оно будет запрашивать у обладателей данных обезличенные наборы сведений, а не персональные данные в чистом виде.

Например, могут затребовать у банков агрегированные транзакции, у операторов связи — статистику по звонкам и т. д., но всё в таком виде, чтобы нельзя было вычислить конкретного человека. Формировать «составы данных» из биометрических персональных данных при этом запрещено — закон прямо исключает обезличивание биометрии для этой ГИС.

Законодатель уделил внимание защите прав граждан при таком обмене данными. Введён механизм уведомления граждан о планируемой передаче их сведений даже в обезличенном виде, с правом возражения. То есть человеку должны сообщить, что сведения о нём (пусть и обезличенные) могут быть переданы, и он вправе запретить это — тогда передачу отменят.

Кроме того, доступ к обезличенным данным в ГИС получат только доверенные лица и организации: ни иностранные компании, ни организации с неопределённым статусом собственности, ни люди с судимостями за киберпреступления допущены не будут. Это сделано для снижения рисков утечек и злоупотреблений при дальнейшем использовании обезличенных данных.

Новые правила обезличивания данных требуют от организаций заблаговременной подготовки. Операторам персональных данных уже сейчас рекомендуется начать приводить свои процессы в соответствие с грядущими изменениями.

- ✓ **Разработать или обновить внутренние политики и инструкции.** Разработать (обновить) локальный акт, регламентирующий порядок обезличивания ПД. В документе следует прописать: какие данные подлежат обезличиванию, в каких случаях; какими методами вы их обезличиваете; как оцениваете достаточность обезличивания; как храните обезличенные данные и т. д. Также вносятся изменения в Политику обработки ПД, добавляя положения об анонимизации.
- ✓ **Определить и внедрить подходящие методы обезличивания**. Проанализируйте, какие из официально утверждённых методов лучше подходят под ваши наборы данных.
- ✓ **Закрепить методы во внутренних актах.**

КОМПАС ЛИДЕРА

- ✓ **Настроить раздельное хранение данных. Проверьте архитектуру ваших информационных систем:** оригинальные персональные данные и обезличенные должны храниться раздельно.
- ✓ **Назначить ответственных за работу с ГИС обезличенных данных**. Если ваша организация подпадает под вероятные требования (например, вы оператор больших массивов клиентских данных), целесообразно определить сотрудника или подразделение, которое будет отвечать за взаимодействие с государственной платформой ЕИП НСУД.
- ✓ **Обучить персонал и обновить договоры**.

Обезличивание ПДн является обязательным только в случае получения требования Минцифры о предоставлении обезличенных данных в ЕИП НСУД.

Скорее всего, в первую очередь запросы на передачу обезличеных данных начнут поступать крупным компаниям, располагающим большим количеством ПДн: операторам сотовой связи, сетевым ритейлерам, крупным производителям, перевозчикам и др.

На малый бизнес / ИП внимание, скорее всего, будет обращено значительно позже, хотя такие запросы тоже обязательно будут.

Во всех остальных случаях обезличивание является добровольным сознательным выбором оператора ПДн для решения определенных задач.

Например:

- ✓ по завершении цели обработки ПД / как альтернатива уничтожению данных;
- ✓ при передаче обезличенных ПДн третьим лицам без согласия клиента (когда получить согласие клиента на передачу обычных ПДн не представляется возможным);
- ✓ обезличивание для использования ПДн в новых целях;
- ✓ обезличивание при обработке видеозаписей и биометрии, когда получить согласие третьих лиц не представляется возможных (публичная видеосъемка и др.).

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

КОМПАС ЛИДЕРА

8 (812) 320-44-22 info@compaslidera.ru compaslidera.ru