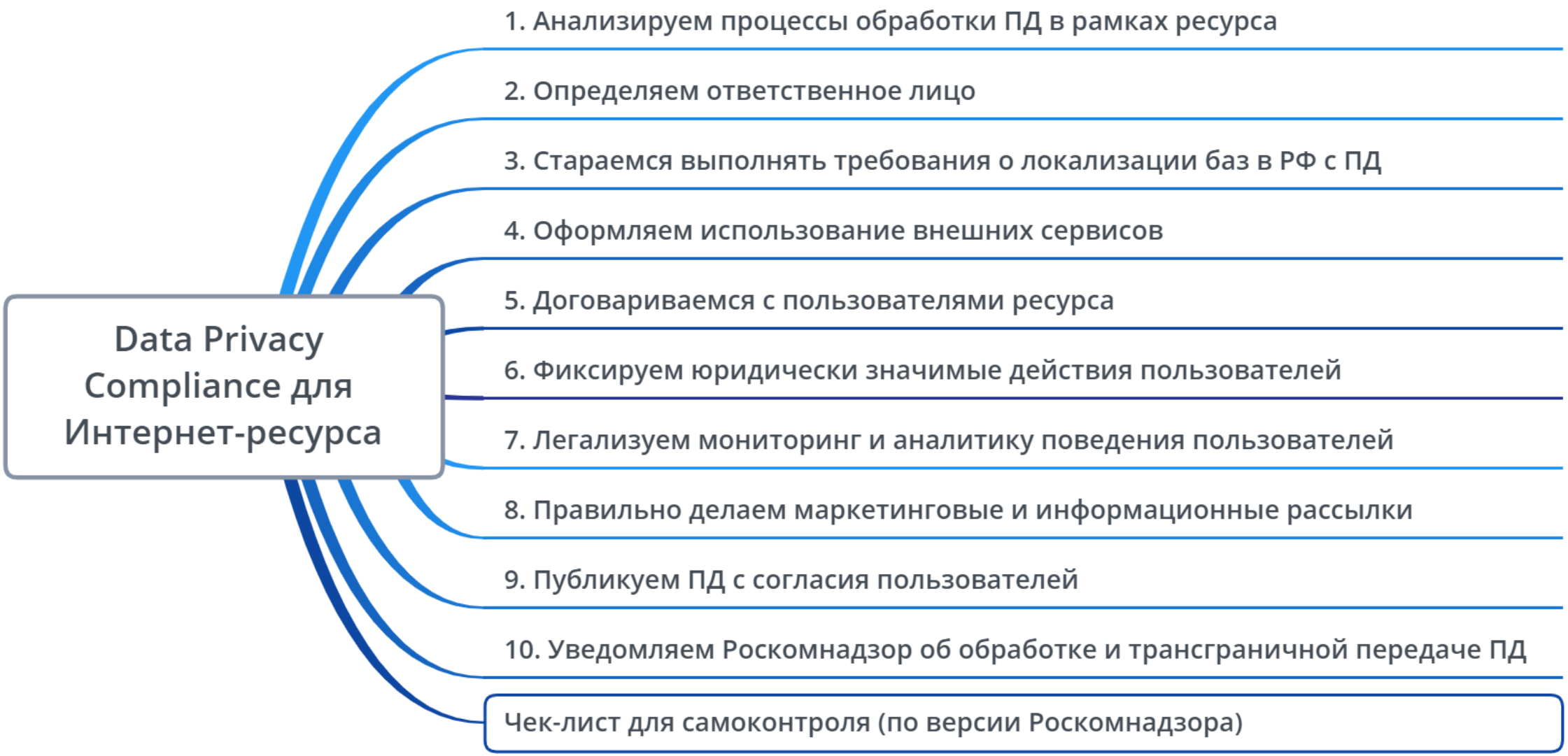
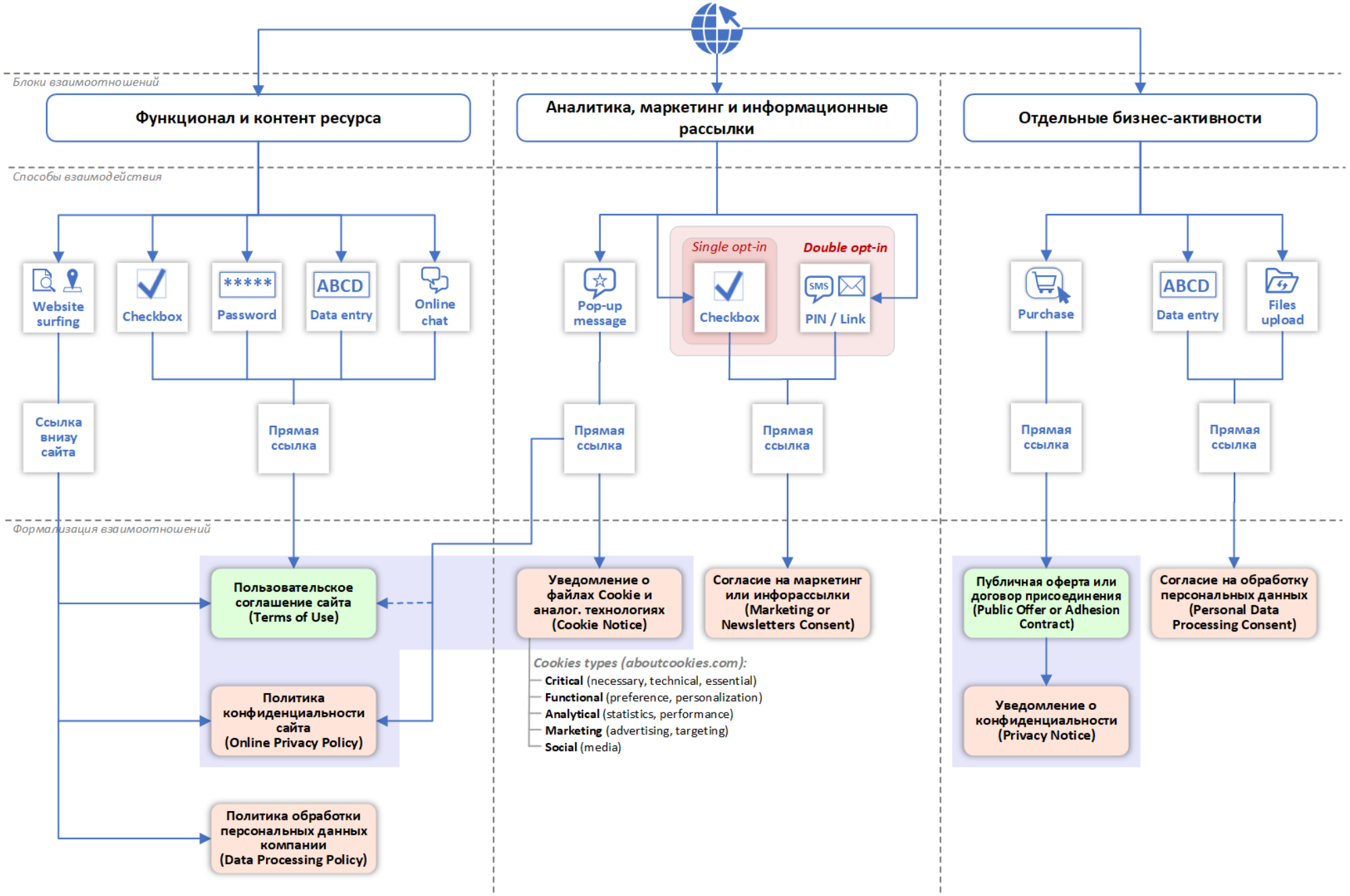
Data Privacy Compliance для Интернет-ресурсов | Алексей Мунтян

10 практических шагов **|** *Редакция от 29.06.2023*

2 10 шагов и самоконтроль



3 Анализируем процессы обработки ПД в рамках ресурса



4 Определяем ответственное лицо

Надзорные органы выясняют принадлежность имущественных и иных прав в отношении:

- доменного имени;
- дизайна и информационных материалов (контента);
- системы управления (CMS) и баз данных;
- информационно-технологической инфраструктуры.

Администратор доменного имени – лицо, на имя которого зарегистрировано предназначенное для сетевой адресации символьное обозначение (доменное имя).

Владелец сайта (ресурса) в сети «Интернет» – лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети Интернет, в том числе порядок размещения информации на таком сайте.

Оператор в отношении ПД – лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПД, а также определяющие цели обработки ПД, состав ПД, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Логика надзорных органов и суда:

администратор домена = владелец сайта = оператор ПД, *пока не доказано обратное*.

Решение Мосгорсуда по делу о блокировке в РФ LinkedIn: ответственность за содержание информации на сайте в сети «Интернет» несет администратор домена, так как использование ресурсов сайта без его контроля невозможно.

5 Стараемся выполнять требования о локализации в РФ баз с ПД

Ч.5 ст.18 152-ФЗ «О персональных данных»:

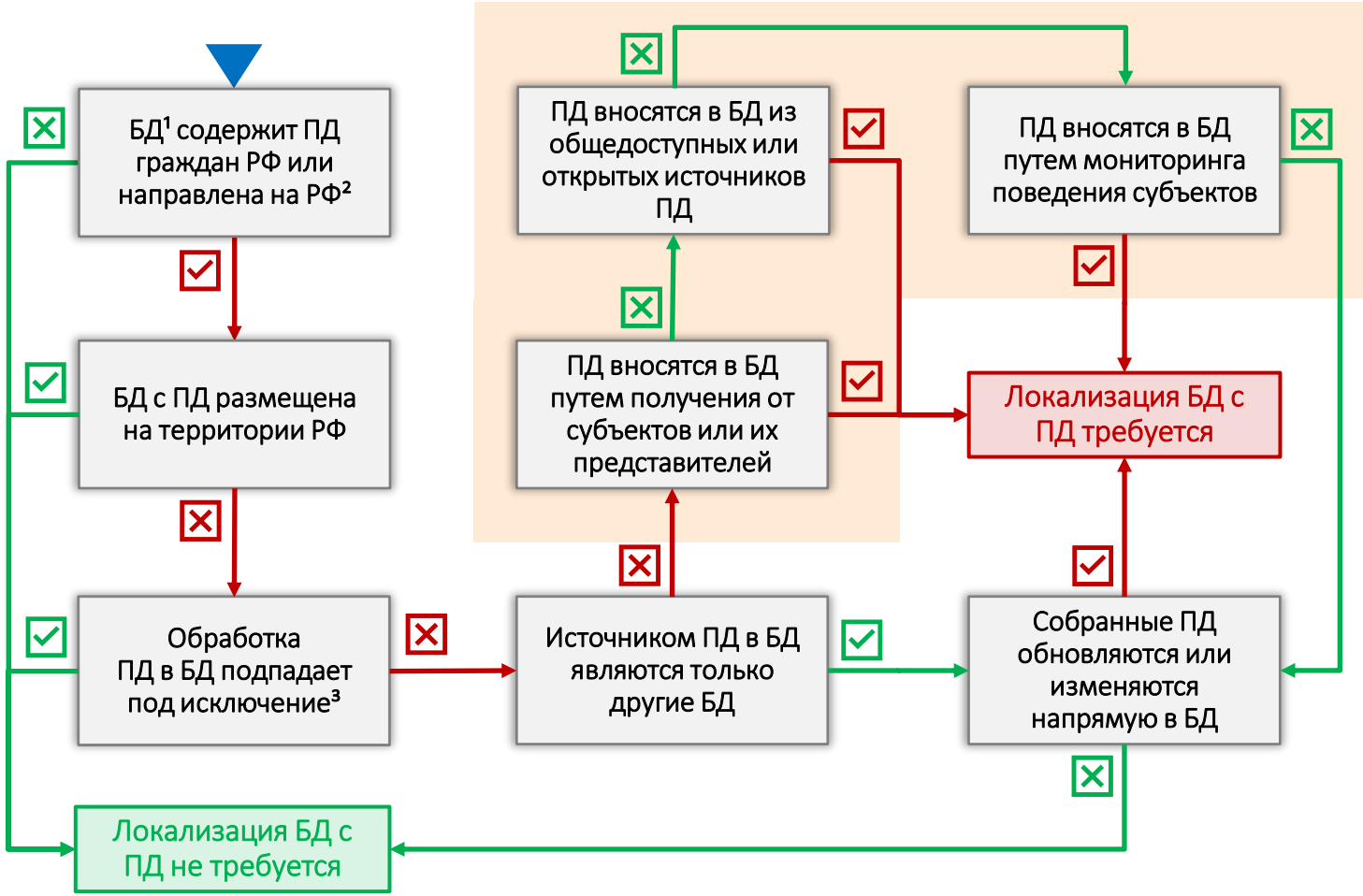
При сборе ПД, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить **запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение** персональных данных **граждан Российской Федерации** с использованием баз данных, находящихся на **территории Российской Федерации**, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона.

Не все ПД нужно локализовывать в РФ:

Получение новых ПД путем использования (анализа) имеющихся в наличии данных, которые ранее были собраны в базы данных на территории РФ и переданы за рубеж, может производиться посредством зарубежных БД и без предварительной локализации в РФ.

Риски применения Google Analytics и аналогов:

Управления Роскомнадзора по Приволжскому федеральному округу и по Курганской области считают нарушением ч.5. ст.18 152-ФЗ применение на сайте Интернет-сервиса «Google Analytics», посредством которого осуществляется обработка персональных данных пользователей сайта с использованием баз данных, находящихся вне территории РФ.



[1] База данных – упорядоченный массив данных, независимый от вида материального носителя информации и используемых средств его обработки (архивы, картотеки, электронные базы данных).

[2] Направленность БД сайта или мобильного приложения на территорию РФ определяется, в том числе:
- адресом сайта в российской доменной зоне (.ru, .рф., .su, whois-service.ru/domains/?id=russian);
- русскоязычной версией пользовательского интерфейса;
- возможностью доставки товара, оказания услуги или пользования цифровым контентом в РФ.

Решение мирового судьи Таганского района по делу сервиса Speedtest.net поставило под сомнение вышеприведенную практику, если на Интернет-ресурсе отсутствуют какие-либо ограничения для прохождения процедуры регистрации российских пользователей.

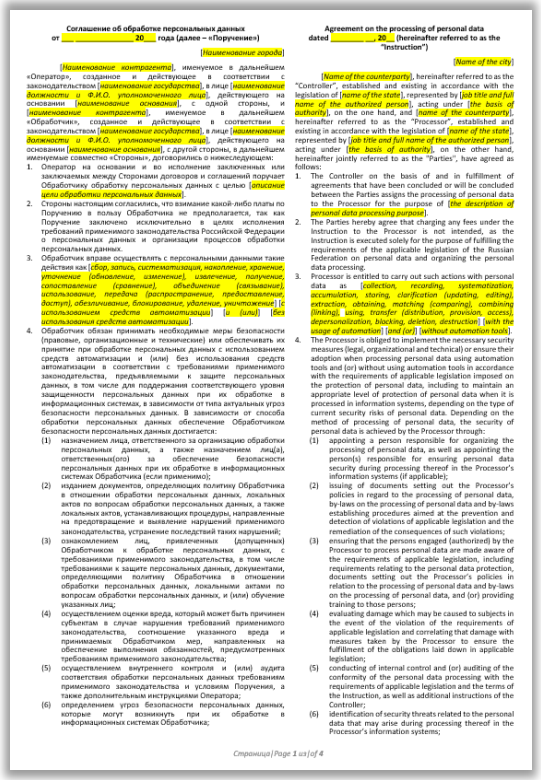
[3] См. п.п. 2, 3, 4, 8 ч.1 ст.6 Федерального закона № 152-ФЗ «О ПД».

6 Оформляем использование внешних сервисов

По мнению Роскомнадзора, необходимость в заключении **соглашения о поручении обработки ПД** возникает в том случае, если оператор ПД, в принципе, способен самостоятельно осуществить обработку ПД, **включая доступ и хранение**, для достижения предусмотренной цели, но в силу различных причин принял решение **делегировать** (полностью или в какой-либо части) **функцию своему контрагенту-«обработчику».**

Поручение обработки ПД при использовании внешних сервисов

- Виртуальный хостинг
- Облачные сервисы (SaaS, PaaS, IaaS)
- Администрирование и поддержка
- IT-безопасность



Соглашение об обработке персональных данных
от «__» _____ 20__ года (далее – «Поручение»)

[*Наименование города*]

[*Наименование контрагента*], именуемое в дальнейшем «Оператор», созданное и действующее в соответствии с законодательством [*наименование государства*], в лице [*наименование должности и Ф.И.О. уполномоченного лица*], действующего на основании [*наименование основания*], с одной стороны, и [*наименование контрагента*], именуемое в дальнейшем «Обработчик», созданное и действующее в соответствии с законодательством [*наименование государства*], в лице [*наименование должности и Ф.И.О. уполномоченного лица*], действующего на основании [*наименование основания*], с другой стороны, в дальнейшем именуемые совместно «Стороны», договорились о нижеследующем:

1. Оператор на основании и во исполнение заключенных или заключаемых между Сторонами договоров и соглашений поручает Обработчику обработку персональных данных с целью [*описание цели обработки персональных данных*].
2. Стороны настоящим согласились, что взимание какой-либо платы по Поручению в пользу Обработчика не предполагается, так как Поручение заключено исключительно в целях исполнения требований применимого законодательства Российской Федерации о персональных данных и организации процессов обработки персональных данных.
3. Обработчик вправе осуществлять с персональными данными такие действия как [*сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, получение, сопоставление (сравнение), объединение (связывание), использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение*] [*с использованием средств автоматизации*] [*и (или)*] [*без использования средств автоматизации*].
4. Обработчик обязан принимать необходимые меры безопасности (правовые, организационные и технические) или обеспечивать их принятие при обработке персональных данных с использованием средств автоматизации и (или) без использования средств автоматизации в соответствии с требованиями применимого законодательства, предъявляемыми к защите персональных данных, в том числе для поддержания соответствующего уровня защищенности персональных данных при их обработке в информационных системах, в зависимости от типа актуальных угроз безопасности персональных данных. В зависимости от способа обработки персональных данных обеспечение Обработчиком безопасности персональных данных достигается:
(1) назначением лица, ответственного за организацию обработки персональных данных, а также назначением лица(а), ответственного(ых) за обеспечение безопасности персональных данных при их обработке в информационных системах Обработчика (если применимо);
(2) изданием документов, определяющих политику Обработчика в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений применимого законодательства, устранение последствий таких нарушений;
(3) ознакомлением лиц, привлеченных [допущенных] Обработчиком к обработке персональных данных, с требованиями применимого законодательства, в том числе требованиями к защите персональных данных, документами, определяющими политику Обработчика в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных лиц;
(4) осуществлением оценки вреда, который может быть причинен субъектам в случае нарушения требований применимого законодательства, соотношение указанного вреда и принимаемых Обработчиком мер, направленных на обеспечение выполнения обязанностей, предусмотренных требованиям применимого законодательства;
(5) осуществлением внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям применимого законодательства и условиям Поручения, а также дополнительным инструкциям Оператора;
(6) определением угроз безопасности персональных данных, которые могут возникнуть при их обработке в информационных системах Обработчика;

Страница | Page 1 из | of 4

Agreement on the processing of personal data
dated «__» _____ 20__ (hereinafter referred to as the "Instruction")

[*Name of the city*]

[*Name of the counterparty*], hereinafter referred to as the "Controller", established and existing in accordance with the legislation of [*name of the state*], represented by [*job title and full name of the authorized person*], acting under [*the basis of authority*], on the one hand, and [*name of the counterparty*], hereinafter referred to as the "Processor", established and existing in accordance with the legislation of [*name of the state*], represented by [*job title and full name of the authorized person*], acting under [*the basis of authority*], on the other hand, hereinafter jointly referred to as the "Parties", have agreed as follows:

1. The Controller on the basis of and in fulfillment of agreements that have been concluded or will be concluded between the Parties assigns the processing of personal data to the Processor for the purpose of [*the description of personal data processing purpose*].
2. The Parties hereby agree that charging any fees under the Instruction to the Processor is not intended, as the Instruction is executed solely for the purpose of fulfilling the requirements of the applicable legislation of the Russian Federation on personal data and organizing the personal data processing.
3. Processor is entitled to carry out such actions with personal data as [*collection, recording, systematization, accumulation, storing, clarification (updating, editing), extraction, obtaining, matching (comparing), combining (linking), using, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction*] [*with the usage of automation*] [*and (or)*] [*without automation tools*].
4. The Processor is obliged to implement the necessary security measures (legal, organizational and technical) or ensure their adoption when processing personal data using automation tools and (or) without using automation tools in accordance with the requirements of applicable legislation imposed on the protection of personal data, including to maintain an appropriate level of protection of personal data when it is processed in information systems, depending on the type of current security risks of personal data. Depending on the method of processing of personal data, the security of personal data is achieved by the Processor through:
(1) appointing a person responsible for organizing the processing of personal data, as well as appointing the person(s) responsible for ensuring personal data security during processing thereof in the Processor's information systems (if applicable);
(2) issuing of documents setting out the Processor's policies in regard to the processing of personal data, by-laws on the processing of personal data and by-laws establishing procedures aimed at the prevention and detection of violations of applicable legislation and the remediation of the consequences of such violations;
(3) ensuring that the persons engaged (authorized) by the Processor to process personal data are made aware of the requirements of applicable legislation, including requirements relating to the personal data protection, documents setting out the Processor's policies in relation to the processing of personal data and by-laws on the processing of personal data, and (or) providing training to those persons;
(4) evaluating damage which may be caused to subjects in the event of the violation of the requirements of applicable legislation and correlating that damage with measures taken by the Processor to ensure the fulfillment of the obligations laid down in applicable legislation;
(5) conducting of internal control and (or) auditing of the conformity of the personal data processing with the requirements of applicable legislation and the terms of the Instruction, as well as additional instructions of the Controller;
(6) identification of security threats related to the personal data that may arise during processing thereof in the Processor's information systems;

[Ссылка на поручение]

Используем сервисы без поручения обработки ПД

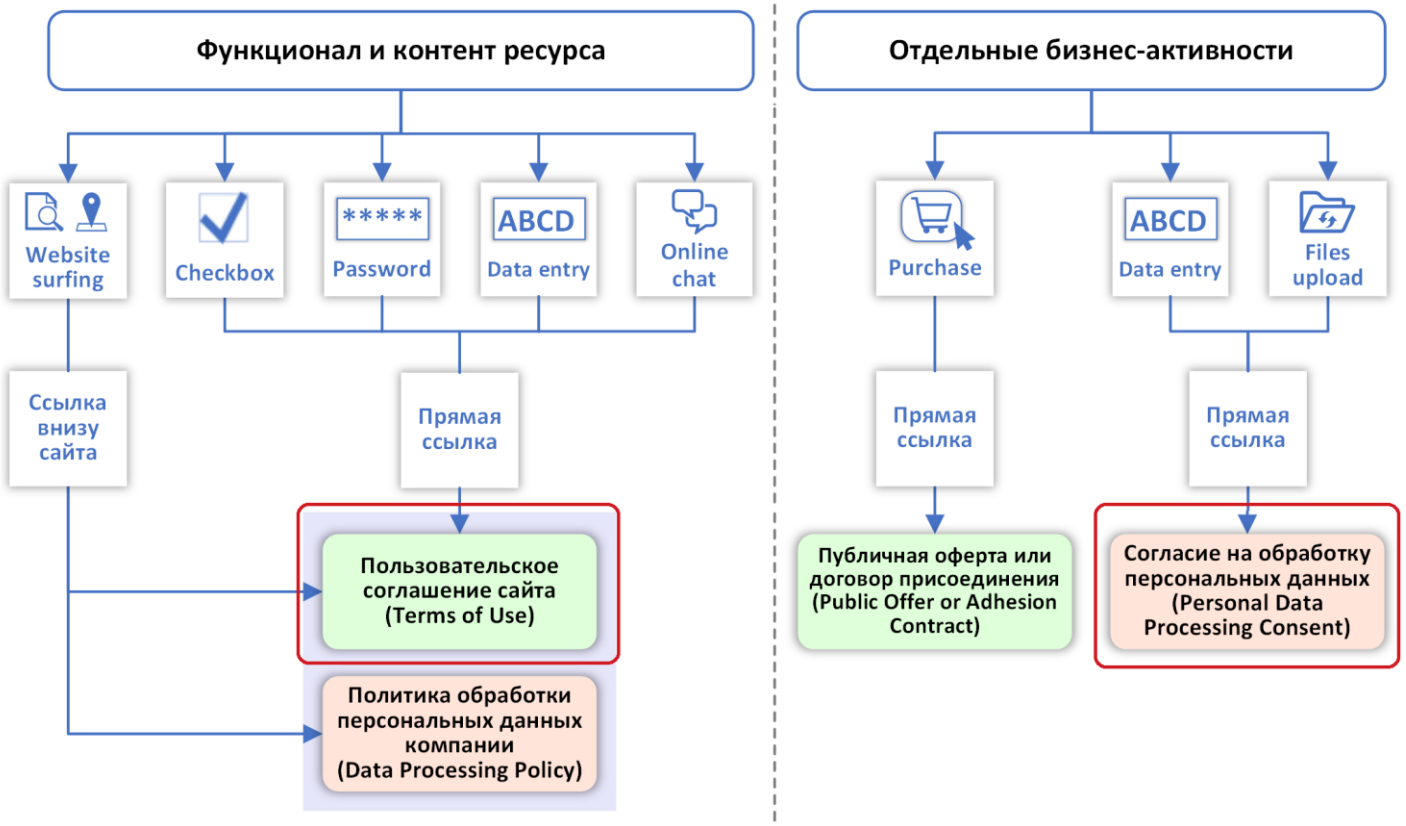
- Чат: *Chatra, Jivosite*
- Авторизация: *LastPass, OneLogin, One Identity*
- Рекомендации: *Foursquare, Yelp*
- Веб-формы: *Google Forms, Яндекс.Формы*
- Опросы: *Typeform, Form.io, Анкетолог, Яндекс.Взгляд*
- Оплата: *Mastercard API, PayPal*
- Медиаконтент: *Youtube, Flickr, Last.fm, Vimeo*
- Безопасность: *PhotoCaptcha, Key Captcha*
- Аналитика: *Google Analytics, Яндекс.Метрика*
- Карты: *Google Maps, Яндекс.Карты*
- Отправка email: *MailGun, Яндекс.Почта*
- Электронная подпись: *SignNow, Контур Диадок*

Риски применения иностранных сервисов:

→признание в качестве трансграничной передачи ПД

→нелокализация сбора ПД российских пользователей

7 Договариваемся с пользователями ресурса



⚠ Не каждую обработку ПД можно легализовать с помощью договора, и тогда нужно получать согласие пользователя в виде отдельного текста.

См. п.2 ч.1 ст.18.1 и ч.ч.3-3.1 ст.22 152-ФЗ, рекомендации Роскомнадзора по составлению Политики конфиденциальности, а также письмо Роскомнадзора о такой Политике с 01.09.2022г.

- Общие положения
- Описание целей обработки ПД
- Для каждой цели обработки ПД указываются:
  - категории и перечень обрабатываемых ПД
  - категории субъектов ПД
  - правовое основание обработки ПД
  - способы обработки и перечень действий с ПД
  - сроки обработки (хранения) ПД
- Порядок актуализации, исправления, уничтожения ПД
- Ответы на запросы субъектов на доступ к ПД

См. п.5 ч.1 ст.5 152-ФЗ: заключаемый с субъектом ПД договор (например, пользовательское соглашение в отношении Интернет-ресурса) не может содержать положения, допускающие в качестве условия заключения договора бездействие субъекта ПД.

Недостаточно показывать пользователю вплывающее при первом посещении Интернет-ресурса сообщение типа «*Продолжая использовать указанный сайт, вы соглашаетесь с условиями…*» (browse-wrap соглашение). Теперь такое сообщение должно содержать:

✓ссылку на полный текст пользовательского соглашения;

✓перечисление действий пользователя, которые будут квалифицироваться как принятие им условий соглашения (например, регистрация на ресурсе, направление сообщений через веб-формы на ресурсе, загрузка размещённых на ресурсе файлов, использование функции ресурса по поиску информации/файлов на ресурсе и т.п.) либо в самом сообщении, либо в виде ссылки на соответствующий пункт пользовательского соглашения.

8 Фиксируем юридически значимые действия пользователей

Я согласен 

Дистанционный договор (согласие) может принимать форму click-wrap соглашения, заключаемого путем щелчка мышью по клавише «я согласен», если это сопровождается текстом такого договора (согласия) и описанием его условий.

Необходимо вести журналирование (логирование) юридически значимые действия пользователей

access_log

```
1 site.ru 195.154.79.109 - - [19/May/2022:06:26:54 +0300] "GET
  /materialy/ HTTP/1.0" 200 41243 "-" "Mozilla/5.0 (Windows NT 10.0;
  Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
2 site.ru 114.119.130.31 - - [19/May/2022:06:28:43 +0300] "GET
  /analitika/ HTTP/1.0" 200 44783 "
3 site.ru 217.76.32.185 - - [19/May/2022:08:34:05 +0300] "GET
  /feed.php?ns=news HTTP/1.0" 200 1588 "-" "Mozilla/5.0 (Windows NT
  10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/101.0.0.0 Safari/537.36"
```

Что нужно принять во внимание:

1. Хотя нет четких требований по составу и периоду хранения логируемой информации, соблюдайте принцип «data minimization»;
2. Обеспечивайте КЦД (*конфиденциальность, целостность и доступность*) логируемой информации;
3. Фиксация логируемой информации может быть квалифицирован как сбор ПД, поэтому для этой цели желательно использовать локализованные в РФ ресурсы (см. Слайд 6).

9 Легализуем мониторинг и аналитику поведения пользователей

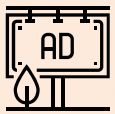
1. Легализовать мониторинг и аналитику поведения пользователей можно с их согласия при первом посещении Интернет-ресурса с помощью всплывающего сообщения (pop-up banner).

2. Простой отсылки на условия Политики конфиденциальности будет недостаточно. Условия согласия на обработку данных детально описываются в отдельном разделе Политики конфиденциальности.

Пример описания условий обработки cookie в Политике конфиденциальности

Тип файла cookie	Владелец	Цель	Срок действия	Как блокировать
Файлы cookie, используемые Оператором (наши файлы cookie)				
Файлы cookie, необходимые для выполнения Сайтом важнейших функций и задач	Оператор	Эти файлы cookie абсолютно необходимы для надлежащей работы Сайта. Они гарантируют его безопасность (аутентификационные файлы cookie) и правильное отображение контента.	Файлы cookie, которые Оператор использует с этой целью, автоматически удаляются с пользовательского устройства через месяц после последнего посещения Сайта.	Пользователь может разрешить или запретить их использование в настройках своего браузера. Поскольку расположение соответствующих настроек зависит от конкретного браузера, более подробные сведения можно найти в справке браузера. Отключение аутентификационных файлов cookie может привести к некоторым неудобствам при использовании Сайта (например, необходимость регулярного прохождения Пользователи процедуры аутентификации на Сайте).
Файлы cookie, используемые поставщиками услуг для Оператора и другими лицами (сторонние файлы cookie)				
Аналитические файлы cookie и технологии	Google Analytics	Эти файлы cookie используются для сбора информации о том, как посетители работают с нашим сайтом. Оператор использует эти сведения для создания отчетов и улучшения сайта. Эти файлы cookie собирают анонимную информацию, в том числе о количестве посетителей сайта, ресурсах, с которых они перешли, и страницах, которые они посмотрели.	Некоторые файлы cookie, создаваемые с этой целью, автоматически удаляются с пользовательского устройства после закрытия браузера. Другие могут храниться до 24 месяцев с момента последнего посещения Пользователем Сайта.	Пользователь может отказаться от отслеживания Google Analytics на странице http://tools.google.com/dlpage/gaoptout?hl=ru-RU.

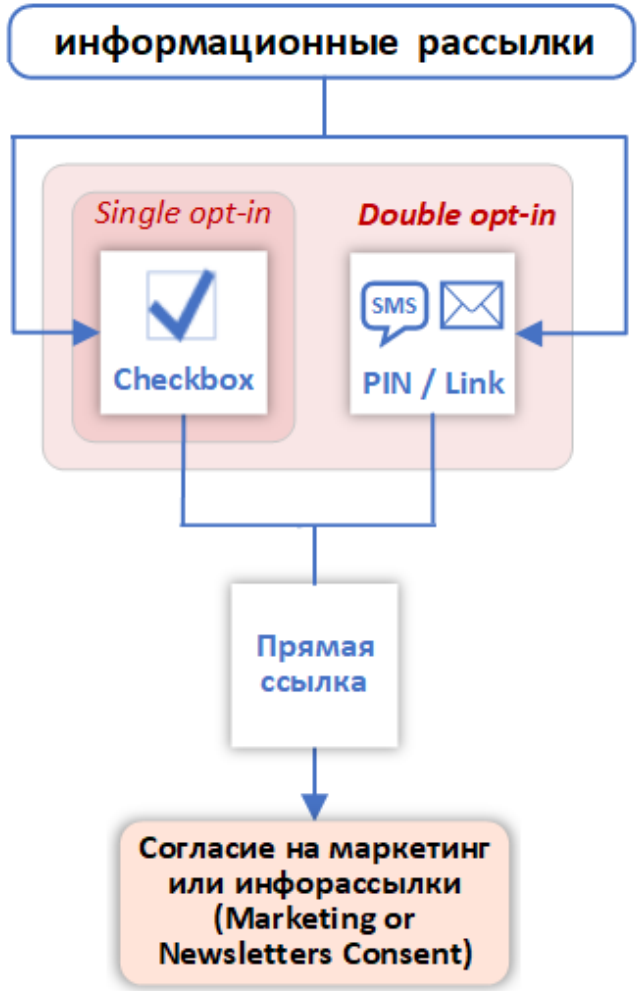
Можно пользоваться рекомендациями Яндекса по легализации сбора персональных данных с использованием Яндекс.Метрика.



Недостатки сервиса анонимизации IP-адресов в Google Analytics:

- применяется только к IP-адресам, но онлайн-идентификаторы cookie или данные пользовательских устройств передаются в открытом виде
- анонимизация IP-адресов происходит только после передачи данных в Google

10 Правильно делаем маркетинговые и информационные рассылки



Механизмы подписки на рассылку

Double Opt-in – пользователь ***дважды активно выражает*** **согласие** на *получение рассылки.* Например, пользователь заполняет форму подписки и нажимает кнопку «Подписаться», а потом на указанный пользователем адрес приходит электронное письмо с просьбой подтвердить согласие на получение рассылки путем нажатия на гиперссылку в письме.

Single Opt-in – пользователь **активно выражает согласие** на *получение рассылки.* Например, пользователь проставляет «галочку» в пустом чек-боксе «Согласен на получение рекламных материалов».

Silent Opt-in – пользователь **пассивно выражает согласие** на *получение рассылки.* Например, «галочка» в чек-боксе «Согласен на получение рекламных материалов» уже предустановлена, а пользователь не убирает её из чек-бокса.

Soft Opt-out – пользователь **в упрощенной форме выражает несогласие** на *получение рассылки.* Например, в условия обслуживания включено согласие пользователя на получение рассылки, а также включен отдельный чек-бокс «Не согласен на получение рекламных материалов», в котором пользователь может проставить галочку.

Hard Opt-out – пользователь **в требующей дополнительных усилий форме выражает несогласие** на *получение рассылки.* Например, пользователю направляется уведомление об обновлении условий обслуживания, в которые теперь включено согласие на получение рассылки, и пользователь в установленный срок направляет отказ от принятия новых условий.

Информационное письмо Банка России № ИН-06-59/70, ФАС России № АК/75514/21 от 06.09.2021 «**О согласии на получение рекламы»**

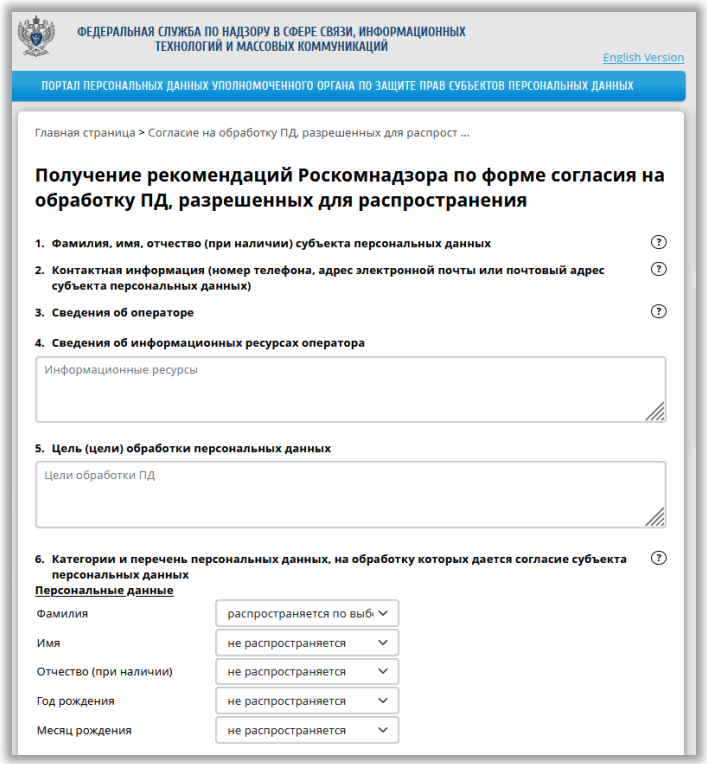
Письмо (недействующее) ФАС России от 11.11.2019 №ДФ/98054/19 «О надлежащих доказательствах при выявлении нарушения требований ч.1 ст.18 Федерального закона "О рекламе"»

На что подписчик email-рассылки может пожаловаться в ФАС и как этого избежать.

Публикуем ПД с согласия пользователей

С 01.03.2021г. размещение (публикация) ПД на разделах (страницах) информационного ресурса, открытых для любого пользователя, требует предварительного получения согласия субъекта на распространение его данных.

Рекомендательный сервис Роскомнадзора по подготовке согласия на распространение ПД
pd.rkn.gov.ru/soglasiya/



Пример согласия на распространение ПД:
rppa.ru/_media/analitika/srpd.docx

Вместе с опубликованными ПД может потребоваться дисклеймер (см. ч.10 ст.101. 152-ФЗ):

Персональные данные распространяются с разрешения субъекта для цели [….]. Условия и запреты субъекта на обработку таких данных неограниченным кругом лиц установлены следующие: [….].

12 Уведомляем Роскомнадзор об обработке и трансграничной передаче ПД

https://pd.rkn.gov.ru/operators-registry/notification/form/

5 Уведомление Роскомнадзора о начале обработки данных

Сообщать в Роскомнадзор нужно, если вы обрабатываете:

1. Данные работников (претендентов) в соответствии с Трудовым кодексом РФ
2. Данные обрабатываются для заключения или исполнения договора с субъектом персональных данных
3. Данные членов общественных объединений (фондов, партий, движений) и религиозных организаций
4. Распространяете персональные данные с согласия субъекта ПД
5. Только ФИО или обработка осуществляется для целей пропуска на территорию
6. Данные, включенные в ИСПД, поименованных в федеральных законах

https://pd.rkn.gov.ru/cross-border-transmission/

6 Трансграничная передача данных (ТПД)

Если оператор ПД осуществлял ТПД до начала вступления данного закона в силу, то он должен:

- Направить уведомление об осуществлении трансграничной передачи в Роскомнадзор
- Предоставить в Роскомнадзор правовые основания для обработки данных в соответствии со ст. 6 152-ФЗ (согласие, договор и т. д.)

Что делать не нужно?

- Получать от субъекта ПД согласие в письменной форме
- Приостанавливать деятельность на время рассмотрения уведомления Роскомнадзором

Приказ Роскомнадзора от 28.10.2022 № 180 "Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных"

13 Чек-лист для проверки Интернет-ресурса

Риски

Ранжирование возможных нарушений, определяемых исходя из позиции и практики Роскомнадзора

высокие

низкие

- → сбор ПД граждан РФ при нахождении БД Интернет-ресурса (хостинг-провайдера) за пределами РФ
- → сбор ПД в зарубежные БД посредством иностранных метрических программ *(например, Google Analytics)*
- → сбор ПД в зарубежные БД посредством сторонних веб-форм или сервисов
- → нет документа, определяющего политику в отношении обработки ПД (далее – «Политика»)
- → отсутствие ссылки на Политику на страницах, где предполагается сбор ПД
- → нет согласия на предоставление ПД неограниченному кругу лиц с использованием Интернет-ресурса
- → нет согласия на обработку ПД, когда такое согласие необходимо *(например, при использовании аналитических и рекламных файлов cookie, а также для целей прямого маркетинга)*
- → согласие на обработку ПД есть, но нет ссылки на его текст или вместо согласия дается ссылка на Политику, из которой нельзя однозначно установить содержание согласия *(цель и иные условия обработки ПД)*
- → отсутствие в Политике сведений о трансграничной передаче ПД при нахождении Интернет-ресурса за пределами РФ и/или при использовании иностранных метрических программ и сервисов *(например, Google Fonts)*
- → несоответствие объема ПД, собираемого веб-формой, положениям Политики
- → наличие ссылок на сторонние веб-формы сбора ПД (в т.ч. иностранные) без указания на это в Политике
- → мониторинг поведения пользователей без указания на это в Политике
- → отсутствие в Политике детального описания обработки ПД для каждой цели
- → отсутствие в Политике описания порядка прекращения обработки (уничтожения) ПД
- → избыточность объема собираемых ПД по отношению к заявленным целям их обработки
- → условием заключения пользовательского соглашения на Интернет-ресурсе является бездействие пользователя
- → обработка и трансграничная передача ПД на Интернет-ресурсе без подачи в Роскомнадзор уведомления

Дополнительно см. ТГ-канал Роскомнадзора

Благодарю за ваше внимание

Алексей Мунтян, *15 лет в Data Privacy*

Основатель и CEO в компании Privacy Advocates

Соучредитель и член Правления в Russian Privacy Professionals Association - RPPA.ru

Внешний Data Protection Officer в четырех транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru