**Структура Политики в отношении обработки персональных данных**

Ведомство рекомендует предусмотреть в документе шесть основных блоков.

**1. Общие цели**

В этом разделе вы фактически отвечаете на вопрос — для чего предназначена Политика в отношении обработки персональных данных? Здесь же разъясняются основные понятия, которые используются в документе, а также права и обязанности оператора и субъекта персональных данных.

**2. Цели сбора персональных данных**

[Ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ](https://normativ.kontur.ru/document?moduleId=1&documentId=395751&p=1210&utm_source=google&utm_medium=organic&utm_referer=www.google.com&utm_startpage=kontur.ru%2Farticles%2F4871&utm_orderpage=kontur.ru%2Farticles%2F4871#h203) (далее — Закон о персональных данных) требует определения конкретных, законных целей сбора данных. Следовательно, нельзя обрабатывать персональные данные, которые не соответствуют этим целям.

Роскомнадзор указывает на то, что цели обработки персональных данных формулируются с учетом:

* анализа правовых актов, регламентирующих деятельность компании;
* целей фактически осуществляемой деятельности;
* деятельности, которая предусмотрена учредительными документами;
* конкретных бизнес-процессов в конкретных информационных системах персональных данных (по структурным подразделениям и их процедурам в отношении определенных категорий субъектов персональных данных).

**3. Правовые основания обработки персональных данных**

Закон о персональных данных не является правовым основанием обработки данных. Эту роль выполняют правовые акты, в соответствии с которыми компания, как оператор, обрабатывает данные.

Таким образом, в Политике в качестве правовых оснований можно указать:

* федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью оператора;
* уставные документы компании;
* договоры, заключаемые между оператором и субъектом персональных данных;
* согласие на обработку персональных данных.

**4. Объем и категории обрабатываемых данных, категории субъектов персональных данных**

Важно, чтобы объем обрабатываемых персональных данных не расходился с заявленными целями обработки.

К категориям субъектов персональных данных могут относиться:

* сотрудники — как настоящие, так и бывшие;
* кандидаты на вакансии;
* родственники работников;
* клиенты и контрагенты (физлица);
* представители или работники клиентов и контрагентов.

Роскомнадзор обращает внимание на то, что по каждой категории субъектов и применительно к конкретным целям следует указать все обрабатываемые персональные данные. Отдельно описываются все случаи обработки специальных категорий персональных данных и биометрических персональных данных (если применяются).

**5. Порядок и условия обработки персональных данных**

В этом разделе нужно указать перечень действий с персональными данными, способы и сроки обработки данных.

Если в рамках достижения целей обработки персональных данных оператор взаимодействует с третьими лицами, то ему нужно:

* пояснить условия передачи персональных данных в адрес третьих лиц (речь идет в том числе о трансграничной передаче данных);
* указать наименование и местонахождение третьих лиц;
* обозначить цели передачи данных и их объем;
* перечислить действия по обработке, способы и иные условия обработки, включая требования к защите обрабатываемых данных.

Передавать персональные данные оператор вправе органам дознания и следствия, а также иным уполномоченным органам по предусмотренным законодательством основаниям.

В Политику следует внести сведения о соблюдении требований конфиденциальности персональных данных (они названы в [ст. 7 Закона о персональных данных](https://normativ.kontur.ru/document?moduleId=1&documentId=395751&p=1210&utm_source=google&utm_medium=organic&utm_referer=www.google.com&utm_startpage=kontur.ru%2Farticles%2F4871&utm_orderpage=kontur.ru%2Farticles%2F4871#h205)) и информацию о принятии мер ([ч. 2 ст. 18.1](https://normativ.kontur.ru/document?moduleId=1&documentId=395751&p=1210&utm_source=google&utm_medium=organic&utm_referer=www.google.com&utm_startpage=kontur.ru%2Farticles%2F4871&utm_orderpage=kontur.ru%2Farticles%2F4871#h325), [ч. 1 ст. 19](https://normativ.kontur.ru/document?moduleId=1&documentId=395751&p=1210&utm_source=google&utm_medium=organic&utm_referer=www.google.com&utm_startpage=kontur.ru%2Farticles%2F4871&utm_orderpage=kontur.ru%2Farticles%2F4871#h219)).

[**Вовремя примите меры по защите персональных данных**](https://kontur.ru/security/features/personal-data?utm_source=google&utm_medium=organic&utm_from=adv-link-enquiry-security-27770-3127)

Кроме того, оператору нужно указать условие прекращения обработки персональных данных. Это может быть достижение целей обработки, истечение срока действия согласия на обработку, отзыв согласия субъекта персональных данных на обработку, выявление неправомерной обработки данных.

Отдельное внимание стоит уделить такому вопросу, как хранение персональных данных. Во-первых, обязательно называются сроки. Во-вторых, используются базы данных, находящиеся на территории РФ. В-третьих, учитывается тот факт, что хранение должно осуществляться в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки. В-четвертых, необходимо упомянуть об иных условия хранения, в том числе, при обработке данных без использования средств автоматизации.

**6. Актуализация, исправление, удаление и уничтожение данных, ответы на запросы субъектов на доступ к персональным данным**

Согласно[ст. 21](https://normativ.kontur.ru/document?moduleId=1&documentId=395751&p=1210&utm_source=google&utm_medium=organic&utm_referer=www.google.com&utm_startpage=kontur.ru%2Farticles%2F4871&utm_orderpage=kontur.ru%2Farticles%2F4871#h221), персональные данные должны быть актуализированы оператором, если подтвержден факт неточности. То же касается и подтверждения факта неправомерности обработки.

Персональные данные подлежат уничтожению при достижении целей их обработки и в случае отзыва субъектом согласия на их обработку, если: иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных; иное не предусмотрено иным соглашением между оператором и субъектом персональных данных. Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами.

На основании [ст. 20](https://normativ.kontur.ru/document?moduleId=1&documentId=395751&p=1210&utm_source=google&utm_medium=organic&utm_referer=www.google.com&utm_startpage=kontur.ru%2Farticles%2F4871&utm_orderpage=kontur.ru%2Farticles%2F4871#h220)оператор обязан сообщить субъекту персональных данных информацию об осуществляемой им обработке по запросу.

Роскомнадзор рекомендует включить в Политику регламенты реагирования на запросы и обращения субъектов персональных данных по поводу неточности данных, неправомерности их обработки, отзыва согласия и доступа к своим данным. Не лишним будет добавить в Политику соответствующие формы запросов и обращений.