**Алгоритм приведения деятельности операторов, уполномоченных лиц в соответствие с требованиями Закона Республики Беларусь от 7 мая 2021 г. № 99-З ”О защите персональных данных“**

**1. Назначение структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных, определение его должностных обязанностей, утверждение положения об организации внутреннего контроля за обработкой персональных данных.**

К основным функциям такого ответственного лица (структурного подразделения) целесообразно отнести, в частности, следующие:

* осуществление (участие в осуществлении) внутреннего контроля за обработкой персональных данных (в этих целях целесообразно утвердить соответствующее положение);
* консультирование руководителя и работников по вопросам применения законодательства о персональных данных;
* участие в разработке (поддержании в актуальном состоянии) документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных;
* ведение (координация ведения) реестра обработки персональных данных или иного документа, систематизирующего обработку персональных данных;
* участие в обучении работников и иных лиц, непосредственно осуществляющих обработку персональных данных по вопросам защиты персональных данных (в том числе разработка тестовых и иных заданий, их проверка и т.п.);
* участие в рассмотрении заявлений, жалоб субъектов персональных данных;
* участие во взаимодействии с уполномоченным органом по защите прав субъектов персональных данных – Национальным центром защиты персональных данных Республики Беларусь.

Варианты назначения:

* освобожденный работник (отдельное структурное подразделение);
* возложение дополнительных функций на одного работника организации;
* возложение дополнительных функций на нескольких работников.

Нецелесообразно:

* возложение функций исключительно на специалиста по информационной безопасности;
* назначение ответственных в каждом структурном подразделении.

Конкретные квалификационные требования к работникам, на которых возлагаются функции лица, ответственного за осуществление внутреннего контроля, Законом не определены. Однако принимая во внимание стоящие перед ним задачи, такое лицо должно назначаться c учетом знания законодательства о персональных данных и практики его применения, понимания бизнес-процессов оператора (уполномоченного лица), в которых используются персональные данные, наличия представления об используемых оператором (уполномоченным лицом) информационных системах, их защите, а также способности выполнять упомянутые функции.

Важно обратить внимание, что в связи с назначением лица, ответственного за осуществление внутреннего контроля, ни оператор, ни уполномоченное лицо, ни работники организации, непосредственно осуществляющие обработку персональных данных, не освобождаются от ответственности, предусмотренной законодательными актами, за допущенные ими нарушения.

**2. Выявление и фиксация бизнес-процессов, в которых используются персональные данные.**

С целью осуществления надлежащего контроля за обработкой персональных данных оператором (уполномоченным лицом) необходимо осуществить систематизацию и учет видов обработки персональных данных в конкретной организации. Без этого невозможно обеспечить реализацию положений статьи 4 [Закона Республики Беларусь   
от 7 мая 2021 г. № 99-З ”О защите персональных данных“](https://pravo.by/document/?guid=12551&p0=H12100099&p1=1&p5=0) (далее – Закон) и реализовать права субъектов персональных данных, например, право на получение информации об обработке персональных данных.

Для указанной цели может быть использован реестр обработки персональных данных или иная форма систематизации видов обработки. Реестр обработки персональных данных может включать:

* цель обработки;
* подразделение (лицо), ответственное за обработку;
* категории лиц, чьи персональные данные обрабатываются;
* категории обрабатываемых персональных данных;
* правовую основу обработки;
* источник получения персональных данных;
* категории получателей персональных данных;
* срок хранения персональных данных.

Структура реестра обработки персональных данных или иного документа, систематизирующего обработку персональных данных, может определяться оператором (уполномоченным лицом). При этом важно не только создать реестр обработки персональных данных или иной документ, систематизирующий обработку персональных данных, но и поддерживать его в актуальном состоянии.

**3. Анализ бизнес-процессов, в которых используются персональные данные, на предмет соответствия требованиям законодательства о персональных данных.**

После выявления и фиксации бизнес-процессов, в которых используются персональные данные, необходимо провести анализ обработки на предмет соответствия требованиям законодательства о персональных данных.

В частности, могут рассматриваться следующие вопросы:

1) формулирование целей обработки персональных данных, в том числе в целях обеспечения их конкретного характера. Распространенная ошибка – указание общих целей, не позволяющих четко определить предмет обработки и круг персональных данных, требующихся для ее достижения;

2) определение правовых оснований для обработки персональных данных исходя из цели обработки. Распространенная ошибка – смешение договора и согласия как самостоятельных правовых оснований обработки посредством включения согласия в текст договора и лишение субъекта персональных данных выбора – давать согласие на обработку или нет;

3) оценка соразмерности и избыточности обрабатываемых персональных данных по отношению к цели обработки. Распространенное нарушение – обработка персональных данных, которые не являются необходимыми для цели обработки (например, обработка информации о родственниках, идентификационном номере при рассмотрении резюме);

4) соответствие получаемых согласий на обработку персональных данных требованиям статьи 5 Закона, если обработка осуществляется на основании согласия. Распространенное нарушение – непредоставление субъекту необходимой информации, указанной в статье 5 Закона, включение согласия в текст договора без возможности выбора – давать согласие на обработку или нет;

5) определение сроков хранения персональных данных исходя из целей обработки. В качестве ориентира при определении сроков хранения персональных данных можно использовать постановление Министерства юстиции Республики Беларусь от 24 мая 2012 г. № 140 ”О перечне типовых документов Национального архивного фонда Республики Беларусь“. В случае, если сроки хранения не установлены законодательством, установление (уточнение) соответствующего срока осуществляется оператором;

6) наличие правовых оснований для предоставления персональных данным уполномоченным лицам. В случае их привлечения к обработке, взаимоотношения между оператором и уполномоченным лицом определяются в соответствии с пунктом 1 статьи 7 Закона.

При отсутствии правовых оснований для обработки, превышении срока хранения, избыточности обрабатываемых персональных данных они подлежат удалению. В случае отсутствия технической возможности удаления персональных данных необходимо принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование.

**4. Издание документов, определяющих политику в отношении обработки персональных данных и обеспечение неограниченного доступа, в том числе с использованием глобальной компьютерной сети Интернет к данной политике.**

Это может быть либо один общий документ, определяющий политику оператора (уполномоченного лица) в отношении обработки персональных данных в виде отдельного (самостоятельного) документа, либо несколько документов, определяющих с учетом специфики (особенностей) деятельности оператора (уполномоченного лица) порядок обработки персональных данных в определенных сферах или в связи с определенными бизнес-процессами (например, в рамках обработки персональных данных на сайте, обработки персональных данных работников и т.п.).

При этом следует обеспечить соотносимость информации о целях, правовых основаниях обработки и круге обрабатываемых персональных данных, а также написание документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных, простым и доступным языком.

Рекомендации по написанию оператором (уполномоченным лицом) документов, определяющих политику в отношении обработки персональных данных размещены в открытом [доступе](https://etalonline.by/document/?regnum=u02103200&q_id=4273220).

**5. Разработка иных (кроме определяющих политику в отношении персональных данных) документов:**

* порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе).

Данный порядок может включать следующую информацию:

1) описание круга персональных данных и категорий работников, которые имеют доступ к таким персональным данным в связи со своими должностными обязанностями;

2) порядок доступа к персональным данным в иных случаях;

3) порядок прекращения доступа работников к обработке персональных данных и т.п.;

* перечня информационных ресурсов (систем), содержащих персональные данные, собственником (владельцем) которых он является, а также категорий персональных данных, подлежащих включению в данные ресурсы (системы).

К таким ресурсам (системам) следует относить, в том числе, такие распространенные ресурсы (системы), как корпоративная электронная почта, программное обеспечение для ведения бухгалтерского учета и отчетности, сайты организаций, автоматизированные системы контроля и управления доступом, системы видеонаблюдения в организации, системы электронного документооборота и т.п.

Категории персональных данных, подлежащих включению в такие ресурсы (системы), определены в подпункте 3.5 пункта 3 [Указа Президента Республики Беларусь от 28 октября 2021 г. № 422 ”О мерах по совершенствованию защиты персональных данных“](https://pravo.by/document/?guid=12551&p0=P32100422&p1=1). С учетом классификации информационных ресурсов (систем), содержащих персональные данные, такие категории предопределяют круг предъявляемых к информационным ресурсам требований по технической и криптографической защите персональных данных.

В случае, если персональные данные содержатся в нескольких информационных ресурсах (системах), то подлежат применению требования к системе защиты информации, устанавливающие более высокий уровень защиты;

* форм согласия субъектов персональных данных применительно к обработке персональных данных на основании согласия. Важно учитывать, что для разных целей обработки данные формы могут отличаться (по кругу обрабатываемых персональных данных, сроку хранения, кругу уполномоченных лиц и т.п.);
* договоров между операторами и уполномоченными лицами в соответствии с требованиями статьи 7 Закона либо дополнительных соглашений в отношении таких договоров;
* устанавливающих сроки хранения персональных данных.

Срок хранения персональных данных может быть определен датой или периодом времени либо критерием, используемым для определения такого срока, а если это невозможно – целями обработки персональных данных;

* перечня уполномоченных лиц, если обработка персональных данных осуществляется такими лицами. При этом такой перечень, равно как и сроки хранения персональных данных, могут быть установлены как в виде отдельного документа, так и в документах, определяющих политику оператора в отношении обработки персональных данных, реестре обработки персональных данных;
* порядка удаления (уничтожения) персональных данных.

Удаление персональных данных оформляется и подтверждается актом удаления в случае, если персональные данные содержатся в электронной форме, либо актом уничтожения в случае, если персональные данные содержатся в письменной форме.

Акт удаления (уничтожения) персональных данных разрабатывается в произвольной форме и утверждается руководителем оператора.

**6. Внесение изменений в должностные обязанности лиц, обрабатывающих персональные данные.**

В должностных инструкциях работников, трудовая функция которых в основном связана с обработкой персональных данных в информационном ресурсе (системе) (включая работников кадровых, бухгалтерских служб, работников, ответственных за функционирование информационного ресурса (системы)) могут быть предусмотрены следующие обязанности по соблюдению установленного законодательством о персональных данных и локальными правовыми актами порядка обработки персональных данных:

* разъяснять субъекту персональных данных его права, связанные с обработкой персональных данных;
* получать в необходимых случаях согласие субъекта персональных данных на обработку персональных данных;
* принимать меры по обеспечению достоверности обрабатываемых персональных данных, при необходимости вносить изменения в персональные данные, которые являются неполными, устаревшими или неточными, за исключением случаев, когда иной порядок актуализации персональных данных установлен законодательными актами либо если цели обработки персональных данных не предполагают изменение таких данных в последующем;
* осуществлять контроль за соответствием срока обработки персональных данных заявленным целям, прекращать обработку персональных данных, а также обеспечивать их удаление или блокирование при отсутствии правовых оснований для обработки персональных данных;
* предоставлять и распространять персональные данные только при наличии соответствующего правового основания;
* обеспечивать предоставление субъектам персональных данных информации об их персональных данных, а также о предоставлении их персональных данных третьим лицам, за исключением случаев, предусмотренных Законом и иными законодательными актами;
* обеспечивать доступ к персональным данным в установленном порядке, вести учет такого доступа и случаев предоставления, распространения персональных данных третьим лицам;
* при возникновении при обработке персональных данных спорных вопросов привлекать уполномоченное лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных.

Конкретный перечень таких обязанностей определяется в каждом конкретном случае, исходя из специфики деятельности работника.

В должностных инструкциях остальных работников, обрабатывающих персональные данные, может быть предусмотрена их обязанность ”соблюдать установленный законодательством о защите персональных данных и локальными правовыми актами порядок обработки персональных данных“.

**7. Ознакомление работников и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных.**

Работников оператора (уполномоченного лица) и иных лиц, которые непосредственно обрабатывают персональные данные, необходимо ознакомить с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, а также документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных.

Оператор (уполномоченное лицо) может избрать любой механизм подтверждения ознакомления (например, под роспись в журнале), позволяющий в дальнейшем продемонстрировать выполнение им названной обязанности.

**8. Обучение лиц, непосредственно осуществляющих обработку персональных данных, и лиц, ответственных за осуществление внутреннего контроля за обработкой персональных данных.**

Операторы (уполномоченные лица) организуют не реже 1 раза в 5 лет прохождение обучения по вопросам защиты персональных данных лицами, ответственными за осуществление внутреннего контроля за обработкой персональных данных, а также лицами, непосредственно осуществляющими обработку персональных данных.

Требования к организации обучения по вопросам защиты персональных данных лицами, ответственными за осуществление внутреннего контроля за обработкой персональных данных, а также лицами, непосредственно осуществляющими обработку персональных данных, установлены Указом Президента Республики Беларусь от 28 октября 2021 г. № 422.

[Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 194 ”Об обучении по вопросам защиты персональных данных“](https://pravo.by/document/?guid=12551&p0=T62104892&p1=1&p5=0) определены категории лиц, ответственных за осуществление внутреннего контроля за обработкой персональных данных, а также лиц, непосредственно осуществляющих обработку персональных данных, которые обязаны проходить обучение в Национальном центре защиты персональных данных Республики Беларусь.

Иные лица проходят обучение:

в учреждениях образования, а также в иных организациях, которым предоставлено право реализации образовательной программы повышения квалификации руководящих работников и специалистов, по образовательной программе повышения квалификации руководящих работников и специалистов;

в других организациях по образовательной программе обучающих курсов (лекториев, тематических семинаров, практикумов, тренингов, офицерских курсов и иных видов обучающих курсов);

у оператора (уполномоченного лица) путем изучения установленных требований в области защиты персональных данных и проверки им знаний по вопросам защиты персональных данных (в форме собеседования, опроса, тестирования и других формах контроля знаний).

**9. Реализация организационных и технических мер по обеспечению:**

* возможности отзыва согласия субъекта персональных данных в электронной форме, если согласие субъекта было получено в такой форме;
* подтверждению информации о получении согласия, его форме и условиях, при которых оно было дано (например, сохранение информации о сеансе, во время которого было получено согласие, вместе с копией информации, которая была предоставлена субъекту в это время);
* фиксации и хранения информации о предоставлении, распространении персональных данных третьим лицам;
* дифференцированного доступа к содержанию информационного ресурса (системы) в соответствии с порядком доступа к персональным данным.

**10. Осуществление** **технической и криптографической защиты персональных данных в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.**

В соответствии с абзацем пятым пункта 3 статьи 17 Закона обязательной мерой по обеспечению защиты персональных данных является осуществление технической и криптографической защиты персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

В целях обеспечения надлежащей технической и криптографической защиты персональных данных оператору важно правильно классифицировать в соответствии с [приказом директора Национального центра защиты персональных данных Республики Беларусь   
от 15 ноября 2021 г. № 12](https://etalonline.by/document/?regnum=U621e3028&utm_source=pravoby&utm_medium=article&utm_campaign=zachita_pd&utm_content=link1&utm_term=novost_23112021) содержащиеся в информационном ресурсе (системе) персональные данные. В зависимости от вида персональных данных, содержащихся в информационном ресурсе (системе), будут определяться класс типовой информационной системы и, соответственно, требования к системе защиты информации, а также иные мероприятия по технической и криптографической защите защиты персональных данных.

Вопросы осуществления технической и криптографической защиты персональных данных регламентированы [приказом Оперативно-аналитического центра при Президенте Республики Беларусь   
от 20 февраля 2020 г. № 66 ”О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449“](https://pravo.by/document/?guid=12551&p0=T62004470&p1=1).