**Примерный перечень вопросов и документов (”чек-лист“), изучаемых Центром в ходе осуществления плановых или внеплановых проверок**

1. Размещение данного перечня вопросов и наименований документов (их категорий) (”чек-листа“) осуществлено с целью предоставления операторам (уполномоченным лицам) информации о том, как можно самостоятельно подтвердить исполнение требований Закона Республики Беларусь от 7 мая 2021 г. № 99-З ”О защите персональных данных“ (далее – Закон) и направлено на повышение эффективности принимаемых мер по обеспечению защиты персональных данных, а также на недопущение наиболее типичных нарушений положений законодательства о персональных данных.

Перечень является примерным и неисчерпывающим. При проведении проверки могут изучаться и иные вопросы с учетом специфики бизнес-процессов конкретного оператора, а также мер, принятых им в рамках риск-ориентированного подхода.

2. Меры по обеспечению защиты персональных данных не должны быть формальными.

В этой связи при оценке их эффективности Центром при осуществлении плановых и внеплановых проверок изучается не только содержание документов оператора, свидетельствующих о принятых мерах по обеспечению защиты персональных данных, но и их фактическая реализация (например, в ходе бесед с работниками оператора, анализа его информационных ресурсов (систем).

Так, например, если оператором назначено лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных, определен порядок и план проведения внутреннего контроля, но такие мероприятия не проводились, то Центром по итогам проверки будут зафиксированы формальный подход по реализации данной обязательной меры и недостаточность принятых мер в целом.

3. Приведенные в ”чек-листе“ наименования документов (их категорий), свидетельствующих об исполнении Закона, являются обобщением наиболее часто встречающихся эффективных практик операторов по его соблюдению, сделанным Центром по итогам опыта проведения контрольных мероприятий в течение 3 лет. В этой связи их не следует рассматривать как единственно возможный способ подтверждения реализации положений Закона.

Оператор вправе подтвердить исполнение его положений, принятие необходимых и достаточных мер для защиты персональных данных изданием иных документов (реализацией иных мероприятий), не указанных в данном перечне.

[**Реализация обязательных мер по обеспечению защиты персональных данных, предусмотренных пунктом 3 статьи 17 Закона**](https://cpd.by/zachita-personalnyh-dannyh/operatoru/mery-po-zashchite/)**.**

1. [*Назначение оператором (уполномоченным лицом), являющимся государственным органом, юридическим лицом Республики Беларусь, иной организацией, структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных*](https://cpd.by/populyarnoye-na-sayte/otvety-na-chasto-zadavayemyye-voprosy/) *(абзац второй):*

приказ о назначении структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных;

закрепление должностных обязанностей лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных, либо функций, задач, полномочий структурного подразделения (например, в [должностной инструкции](https://cpd.by/dolzhnostnaja-instrukcija-specialistu-po-vnutrennemu-kontrolju-obrazec/), трудовом договоре, положении о структурном подразделении);

[локальный правой акт](https://cpd.by/porjadok-osushhestvlenija-vnutrennego-kontrolja-za-obrabotkoj-personalnyh-dannyh/), определяющий порядок осуществления внутреннего контроля за обработкой персональных данных. Ежегодно утверждаемые планы осуществления внутреннего контроля с указанием структурных подразделений, подлежащих такому контролю;

документы, подтверждающие эффективность осуществления внутреннего контроля за обработкой персональных данных (например, докладные записки, отчеты по итогам проведения, предложения по совершенствованию деятельности и иные сведения, подтверждающие эффективность его осуществления);

создание оператором (уполномоченным лицом) условий для эффективной реализации данной меры (предоставление необходимых ресурсов, обеспечение независимости при осуществлении внутреннего контроля, исключение (минимизация) при этом конфликта интересов и т.п.).

1. [*Издание оператором (уполномоченным лицом), являющимся юридическим лицом Республики Беларусь, иной организацией, индивидуальным предпринимателем, документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных*](https://cpd.by/storage/2025/04/1-Razjasnenija-po-sostavleniju-dokumentov-opredeljajushhih-politiku-operatora_UL-v-otnoshenii-obrabotki-PD.doc) *(абзац третий):*

отражение в таких локальных правовых актах порядка и условий обработки персональных данных, сведений об уполномоченных лицах, трансграничной передаче персональных данных, прав субъектов персональных данных и механизмов их реализации;

обеспечение соотношения в таких локальных правовых актах целей обработки персональных данных, категорий субъектов, чьи данные подвергаются обработке, перечня обрабатываемых персональных данных, правовых оснований их обработки и сроков хранения;

обеспечение неограниченного доступа, в том числе с использованием глобальной компьютерной сети Интернет, к таким документам до начала обработки.

1. *Ознакомление работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных, а также обучение указанных работников и иных лиц в порядке, установленном законодательством (абзац четвертый):*

подтверждение такого ознакомления (может быть как на бумажных носителях, так и в информационных ресурсах);

подтверждение обучения по вопросам защиты персональных данных лицами, ответственными за осуществление внутреннего контроля за обработкой персональных данных, а также лицами, непосредственно осуществляющими обработку персональных данных, и проведение проверки их знаний по вопросам защиты персональных данных (в форме собеседования, опроса, тестирования и в других формах с отражением сведений о результатах контроля знаний) (может быть как на бумажных носителях, так и в информационных ресурсах);

эффективность реализации рассматриваемой меры (презентации, памятки, тесты и иные материалы, которые использованы для ознакомления (обучения), понимание работниками ”базовых“ положений законодательства о персональных данных и соответствующих локальных правовых актов оператора (уполномоченного лица), а также организация ознакомления (обучения) с учетом трудовой функции таких работников[[1]](#footnote-1)).

1. *Установление порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе) (абзац пятый):*

[локальный правовой акт, определяющий порядок доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе)](https://cpd.by/porjadok-dostupa-k-personalnym-dannym-v-tom-chisle-obrabatyvaemym-v-informacionnom-resurse-sisteme/);

обусловленность предоставления доступа должностными обязанностями работника;

соблюдение установленного порядка доступа к персональным данным, обрабатываемым как в информационном ресурсе (системе), так и на бумажных носителях.

1. [*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*](https://etalonline.by/document/?regnum=t62004470&q_id=4492401) *(абзац шестой):*

документальное подтверждение соответствия системы защиты информации требованиям законодательства об информации, информатизации и защите информации (наличие аттестата соответствия системы защиты информации информационной системы требованиям по защите информации);

проверка правильности отнесения информационной системы к классу типовых информационных систем;

установление соответствия реального состава и структуры объектов информационной системы общей схеме системы защиты информации (проверка соответствия оборудования и средств защиты информации, используемых оператором, общей схеме системы защиты информации).

[**Реализация мероприятий, предусмотренных Указом Президента Республики Беларусь от 28 октября 2021 г. № 422 ”О мерах по совершенствованию защиты персональных данных“:**](https://cpd.by/zachita-personalnyh-dannyh/operatoru/mery-po-zashchite/)

*1) Установление и поддержание в актуальном состоянии:*

*а)* [*перечня информационных ресурсов (систем), содержащих персональные данные, собственником (владельцем) которых является оператор*](https://cpd.by/resursy-soderzhashhih-personalnye-dannye/)*;*

*б) категорий персональных данных, подлежащих включению в такие ресурсы (системы);*

*в) перечня уполномоченных лиц, если обработка персональных данных осуществляется уполномоченными лицами;*

*г) сроков хранения обрабатываемых персональных данных.*

*2) Внесение в информационный ресурс* [*”Реестр операторов персональных данных“*](https://register.cpd.by/) *сведений об информационных ресурсах (системах), содержащих персональные данные, и их актуализация (в случае необходимости).*

Локальные правовые акты, предусматривающие отражение (внесение) указанных сведений или определяющие порядок их внесения, обеспечение их актуальности[[2]](#footnote-2).

*3)* [*обучение в Центре работников и (или) иных лиц, в обязанности которых входит обеспечение информационной безопасности, по образовательной программе повышения квалификации руководящих работников и специалистов по вопросам технической и (или) криптографической защиты информации*](https://cpd.by/obespechenie-bezopasnosti-informacionnyh-tehnologij/)

[**Соблюдение общих требований к обработке персональных данных согласно статье 4 Закона**](https://cpd.by/zachita-personalnyh-dannyh/operatoru/trebovaniya-k-obrabotke/)(оценка осуществляется применительно к каждому бизнес-процессу):

соблюдение требования о соразмерности заявленных целей обработки персональных данных и обеспечении на всех этапах такой обработки справедливого соотношения интересов всех заинтересованных лиц[[3]](#footnote-3);

[наличие правового основания для обработки персональных данных](https://cpd.by/zachita-personalnyh-dannyh/operatoru/pravovye-osnovanija-obrabotki/)[[4]](#footnote-4) (согласие субъекта персональных данных, а в случае обработки персональных данных без согласия – конкретный структурный элемент нормативного правового акта);

конкретность цели обработки персональных данных, ее законность, а также информирование о ней до начала обработки персональных данных;

соответствие содержания и объема обрабатываемых персональных данных заявленной цели их обработки. Неизбыточность обрабатываемых персональных данных по отношению к заявленной цели обработки;

соблюдение определенных в законодательном акте (акте законодательства, принятом в его развитие) либо оператором сроков хранения персональных данных.

[**Обеспечение соблюдения требований законодательства о персональных данных при их обработке на основании согласия (статья 5 Закона)**](https://cpd.by/forma-soglasija-na-obrabotku-personalnyh-dannyh-razrabotana-centrom/)**.**

1) [Подтверждение соответствия согласия трем критериям](https://cpd.by/zachita-personalnyh-dannyh/grajdaninu/soglasiye-na-obrabotku-personalnykh-dannykh/) (для выполнения обязанности, предусмотренной пунктом 7 статьи 5 Закона)[[5]](#footnote-5):

а) свободное;

б) однозначное;

в) информированное (предоставление информации, предусмотренной пунктом 5 статьи 5 Закона, в соответствующей форме выражения согласия, отдельно от иной предоставляемой ему информации).

2) Прекращение обработки персональных данных в случае отзыва согласия либо истечения срока, на который оно давалось (при отсутствии иных оснований для обработки персональных данных).

**Соблюдение требований законодательства о персональных данных при поручении их обработки уполномоченным лицам (статья 7 Закона)** *(на примере договора)***:**

[включение в договор (заключение отдельного соглашения) между оператором и уполномоченным лицом положений, предусмотренных пунктом 1 статьи 7 Закона](https://cpd.by/forma-soglasija-na-obrabotku-personalnyh-dannyh-razrabotana-centrom-2/);

до привлечения уполномоченных лиц к обработке персональных данных осуществление оценки предоставляемых ими гарантий принятия достаточных правовых, организационных и технических мер для обеспечения защиты персональных данных в соответствии с требованиями Закона (наличие порядка оценки предоставления уполномоченными лицами таких гарантий, запросы по данному вопросу (ответы на них), изучение сайта уполномоченного лица, заполнение чек-листов и т.п.);

осуществление контроля за выполнением уполномоченными лицами мер по обеспечению защиты персональных данных, а также обеспечением прекращения обработки персональных данных, их удалением или блокированием при отсутствии оснований для обработки персональных данных (наличие порядка оценки предоставления уполномоченными лицами таких гарантий, закрепление порядка такого контроля в договоре, запросы по данному вопросу (ответы на них), заполнение чек-листов и т.п.).

**Принятие согласно пункту 3 статьи 8 Закона комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при обработке специальных персональных данных для прав и свобод субъектов персональных данных** (осуществление видеонаблюдения за аппаратными средствами, обрабатывающими биометрические персональные данные, охрана таких объектов и т.п.).

[**Соблюдение установленного порядка трансграничной передачи персональных данных на территорию иностранного государства, где не обеспечивается надлежащий уровень защиты прав субъектов персональных данных (статья 9 Закона):**](https://cpd.by/zachita-personalnyh-dannyh/operatoru/transgranichnaya-peredacha/)

информирование субъекта персональных данных о рисках, возникающих в связи с отсутствием надлежащего уровня их защиты (если передача осуществляется на основании согласия);

наличие иных альтернативных каналов передачи персональных данных, которые не сопряжены с рисками, существующими при трансграничной передаче персональных данных в иностранные государства, не обеспечивающие надлежащий уровень защиты прав субъектов персональных данных (если передача осуществляется на основании договора).

[**Реализация прав субъектов персональных данных, предусмотренных статьями 10 – 13 Закона**](https://cpd.by/zachita-personalnyh-dannyh/operatoru/realizacija-prav-subektov-personalnyh-dannyh/)**:**

порядок реализации прав субъектов персональных данных (в случае отсутствия отдельного локального правового акта по данному вопросу изучается его отражение в документах, определяющих политику оператора в отношении обработки персональных данных), его соблюдение (например, фактическое удаление персональных данных после уведомления субъекта персональных данных об их удалении);

заявления субъектов персональных данных и ответы на них (порядок регистрации заявлений, соблюдение установленных сроков их рассмотрения и т.п.);

создание условий для реализации прав субъектов персональных данных (возможность отзыва согласия в той форме, посредством которой оно получено, ведение учета случаев предоставления персональных данных третьим лицам и т.п.).

[**Соблюдение требований законодательства о персональных данных при обработке персональных данных соискателей на трудоустройство, работников и членов их семей**](https://cpd.by/populyarnoye-na-sayte/otvety-na-chasto-zadavayemyye-voprosy/)**:**

порядок обработки персональных данных соискателей на трудоустройство, работников и членов их семей (обеспечение правового основания обработки персональных данных, соблюдения требования о неизбыточности обрабатываемых персональных данных, сроков хранения персональных данных) в информационных ресурсах (системах) оператора, а также на бумажных носителях (например, личные дела работников, должностные инструкции, приказы, заявления работников нанимателю), в том числе путем изучения правил внутреннего трудового распорядка, коллективного договора, соглашений и документов, регламентирующих внутренний трудовой распорядок и иных локальных правовых актов по вопросу производственно-технологической, исполнительской и трудовой дисциплины, предоставления гарантий и компенсаций работникам;

предоставление персональных данных работников иным операторам.

1. При организации ознакомления (обучения) работников, которые получают согласие на обработку персональных данных, следует сделать акцент на разъяснении положений статей 5 и 10 Закона, а работников кадровых и бухгалтерских служб – на правовых основаниях обработки персональных данных без получения согласия, приведя примеры нормативных правовых актов по предмету их деятельности, предусматривающих обязанности (полномочия), для выполнения которых требуется обработка персональных данных. [↑](#footnote-ref-1)
2. В случае большого количества уполномоченных лиц (абзац «в» пункта 1), динамичности или краткосрочности договорных отношений не будет являться нарушением определение локальным правовым актов порядка ведения такого перечня (без его утверждения). [↑](#footnote-ref-2)
3. Примером нарушения в данном случае может являться отсутствие альтернативы обработки биометрических персональных данных как условия доступа в спортивный зал. [↑](#footnote-ref-3)
4. В соответствии с абзацем шестым статьи 1 Закона под обработкой понимается любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных. Особое внимание при проведении проверки уделяется наличию правовых оснований для сбора, хранения, предоставления и распространения персональных данных. [↑](#footnote-ref-4)
5. Если согласие получено в письменной форме, таким подтверждением является документ, подписанный субъектом персональных данных. Если согласие получено в иной электронной форме, при доказывании получения согласия недопустимо ограничиваться хранением в информационном ресурсе (системе) лишь сведений о дате и времени его получения. Следует подтвердить условия, при которых это согласие было получено (в частности, его свободный, однозначный и информированный характер). Это может быть сделано, в частности, путем предоставления описания порядка получения согласия, действовавшего на момент его получения (например, техническое задание на доработку страницы сайта, на которой получается согласие). [↑](#footnote-ref-5)