Приложение
к Разъяснениям об обработке
персональных данных при
осуществлении деятельности
субъектов малого
предпринимательства

ЧЕК – ЛИСТ

по приведению деятельности операторов –
субъектов малого предпринимательства
в соответствие с требованиями Закона

Для кого предназначен чек-лист?

Данный чек-лист предназначен для субъектов малого предпринимательства, к которым относятся:

1. малые организации (со средней численностью работников за календарный год до 100 человек);
2. физические лица, осуществляющие индивидуальную предпринимательскую деятельность:
   2.1. индивидуальные предприниматели;
   2.2. самозанятые;
   2.3. ремесленники;
   2.4. физические лица – субъекты агроэкотуризма.

Для чего предназначен чек-лист?

В чек-листе приведены основные аспекты, которые необходимо учитывать субъектам малого предпринимательства при обработке персональных данных.

Выстраивание субъектами малого предпринимательства надлежащей работы с персональными данными – действенный инструмент:

1. повышения эффективности и конкурентоспособности бизнеса;
2. формирования доверительного отношения граждан к качеству оказываемых услуг и выполняемых работ;
3. снижения трудовых, материальных и технических затрат;
4. минимизации рисков утечки персональных данных (и, как следствие, финансовых и репутационных потерь).

Кроме того, затраты на устранение наступивших негативных последствий зачастую могут значительно превышать как временные, так и финансовые расходы субъектов малого предпринимательства на организацию и проведение превентивных мероприятий по защите информации.

Что такое персональные данные?

Персональными данные – любая информация, относящаяся к идентифицированному физическому лицу или лицу, которое может быть идентифицировано.

Например, к персональным данным можно отнести:

фамилию, имя, отчество, место жительства, дату рождения, идентификационный номер, серию и номер паспорта;

номер телефона физического лица, адрес его электронной почты, данные о его местоположении;

IP-адрес компьютера, история поиска в браузере, история покупок;

занимаемую должность, размер заработной платы работника, служебную характеристику;

информацию о болезнях, визитах к врачу;

данные аккаунтов в социальных сетях;

информацию об участии в программах лояльности, акциях и т.д.;

номер банковского счета (банковской карты) и иные реквизиты, информация о платежах;

фотографии, видео- и аудиозаписи, содержащие изображение или голос, и т.п.

В отдельную категорию выделяются *специальные персональные данные* – информация, касающаяся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности, а также биометрические и генетические персональные данные.

Например, специальными персональными данными являются:

сведения, содержащиеся в больничных листках работников организации;

информация о членстве в профессиональных союзах;

сведения из единого государственного банка данных о правонарушениях, и др.

Важно помнить, что к персональным данным относится не только информация, которая идентифицирует лицо, но и которая *может быть использована для его идентификации*.

Например, адреса электронной почты может быть достаточно, чтобы идентифицировать кого-то, когда в электронном адресе отражаются данные о лице (ФИО, дата рождения, место работы и др.) (например, Kovalev12.10.1983@cpd.by).

При этом для признания сведений персональными данными реальная идентификация человека не требуется. Достаточно наличия соответствующей возможности.

Что понимается под обработкой персональных данных?

Обработка персональных данных – любое действие или совокупность действий, совершаемых с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных.

Например, обработка персональных данных имеет место:

при получении организацией персональных данных потребителей при заполнении ими формы обратной связи на сайте;

при направлении рекламной рассылки с использованием абонентского номера, адреса электронной почты;

при съемке блогерами видеороликов на различную тематику с участием случайных граждан и их последующее размещение в социальных сетях;

при публикации отзывов потребителей на сайте и (или) социальных сетях и т.д.

Кто такой оператор персональных данных?

В качестве оператора может выступать:

1. организация (например, юридическое лицо, относящееся к числу малых организаций);
2. физическое лицо, осуществляющее обработку персональных данных, связанную с индивидуальной предпринимательской деятельностью (самозанятый, индивидуальный предприниматель, ремесленник и др.).

Кто является уполномоченным лицом и в чем его отличие от оператора?

В качестве уполномоченного лица может выступать:

1. организация (юридическое лицо);
2. физическое лицо, осуществляющее обработку персональных данных, связанную с профессиональной или индивидуальной предпринимательской деятельностью.

В отличие от оператора, уполномоченное лицо не определяет ключевые параметры обработки персональных данных (цели и сроки обработки, объем обрабатываемых данных, круг лиц, которым предоставляются персональные данные), а действует от имени или в интересах оператора в соответствии с его поручениями, как правило, за вознаграждение.

Например, распространенной практикой для небольших организаций, индивидуальных предпринимателей является передача части своих функций, связанных с обработкой персональных данных,

на аутсорсинг другой организации (индивидуальному предпринимателю) (ведение бухгалтерского учета, системное администрирование локальной сети, транспортные услуги, IT-поддержка и т.п.).

В большинстве таких случаев исполнитель услуг действует в соответствии с инструкциями (поручениями, указаниями и т.п.) заказчика, закрепленными в договоре, от его имени или в его интересах. В подобных ситуациях заказчик выступает оператором, а исполнитель является уполномоченным лицом.

Какие требования предъявляются к обработке персональных данных?

Если Вы осуществляете обработку персональных данных, важно убедиться в том, что:

1. цель, для которой Вы обрабатываете персональные данные, является законной;
2. Вы обрабатываете только те персональные данные, которые необходимы для достижения заявленной цели;
3. Вы проинформировали субъектов персональных данных о том, как, какие персональные данные и для каких целей будут обрабатываться;
4. у Вас есть надлежащее правовое основание для обработки персональных данных. Если правовым основанием выступает согласие, Вы получили его до начала обработки персональных данных;
5. Вы приняли меры по обеспечению защиты персональных данных субъектов для обеспечения их безопасности и недопущения киберинцидентов, повлекших утечку персональных данных;
6. Вы обеспечиваете достоверность обрабатываемых персональных данных субъектов;
7. Вы храните персональные данные не дольше, чем этого требуют заявленные цели обработки. Если срок хранения определен в законодательстве, то данные могут храниться в течение этого срока.

На каких правовых основаниях может осуществляться обработка персональных данных?

Основаниями обработки персональных данных выступают:

1. согласие субъекта персональных данных;
2. иные основания, предусмотренные статьями 6 и 8 Закона, не требующие получения согласия. В частности:

2.1. если обработка персональных данных осуществляется при оформлении трудовых отношений, а также в процессе трудовой деятельности субъекта персональных данных в случаях, предусмотренных законодательством (например, при трудоустройстве

работник предоставляет ряд обязательных документов согласно законодательству о труде, содержащих персональные данные);

2.2. если целью обработки персональных данных является исполнение заключенного договора (например, информирование (напоминание) субъекта персональных данных о предстоящем визите клиента к специалисту для оказания платной услуги посредством смс-сообщения);

2.3. если обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами (например, индивидуальные предприниматели обязаны вести книгу жалоб и предложений, форма которой установлена законодательством и предусматривает необходимость внесения в нее ряда сведений).

Каким обязательным требованиям должно соответствовать согласие субъекта персональных данных, если оно выступает правовым основанием обработки персональных данных?

Согласие должно быть:

1. *свободным* (субъект должен самостоятельно, исходя из своего внутреннего убеждения, выразить свою волю в отношении обработки персональных данных);

2. *однозначным* (субъект должен дать свое согласие путем совершения четкого намеренного действия);

3. *информированным* (оператор должен простым и ясным языком разъяснить субъекту персональных данных цели обработки персональных данных, кто будет осуществлять обработку персональных данных, сроки обработки, его права, связанные с обработкой персональных данных, механизм реализации таких прав и др.).

Необходимо ли получать согласие на обработку персональных данных при заключении договора (включать соответствующий пункт в содержание такого договора)?

Получение подобного согласия и включение указанных положений в договор является избыточной обработкой персональных данных и противоречит требованиям Закона.

Обработка персональных данных, необходимых для целей заключения договора и исполнения обязанностей, предусмотренных этим договором, осуществляется без согласия субъекта персональных данных на основании абзаца пятнадцатого статьи 6 Закона.

Необходимо ли получать отдельное согласие на каждую цель?

Оператору следует обращаться к субъекту персональных данных за получением отдельного согласия на каждую из целей (принцип ”одна цель – одно согласие“). При этом субъект персональных данных вправе давать свое согласие исключительно на те цели, которые посчитает нужными.

Если в работе используется сайт, какие существуют особенности обработки персональных данных?

Файлы cookie – неотъемлемая часть любого сайта. Они относятся к персональным данным.

Если на сайте обрабатываются только технические файлы cookie, получать согласие субъекта персональных данных (пользователя сайта) не требуется. Согласие необходимо получить на сбор и иную обработку необязательных файлов cookie.

При обработке файлов cookie необходимо избегать следующих типичных нарушений:

отсутствие cookie-баннера;

невозможность отказаться от сбора файлов cookie (cookie-баннер содержит только кнопку ”Ok“, ”Понятно“, ”Согласен“ и т.п.);

cookie-баннер содержит кнопки, которые позволяют согласиться или отказаться от сбора файлов cookie, но доступ к контенту сайта невозможен без совершения выбора относительно сбора файлов cookie;

отсутствие политики обработки файлов cookie;

отсутствие механизма отзыва согласия на обработку файлов cookie;

отказ от обработки файлов cookie намеренно усложнен (например, согласие выражается в один ”клик“, а для отказа от обработки необходимо выбрать нужные опции в нескольких всплывающих один за одним cookie-баннерах);

кнопка отказа от обработки трудноразличима, появляется на cookie-баннере спустя время.

При посещении интернет-ресурса перед пользователем должен появиться cookie-баннер с понятным информационным сообщением, например: ”Для обеспечения удобства пользователей сайта используются cookies“.

При этом на cookie-баннере должна быть не только кнопка ”Принять“, но и ”Отклонить“.

На cookie-баннере может также размещаться кнопка ”Настроить“ (или ”Подробнее“). В настройках пользователь может, например, отключить рекламные файлы cookie, но оставить аналитические, или наоборот.

При этом обращаем внимание, что противоречит принципу прозрачности обработки персональных данных использование ”темных паттернов“, например, выделение цветом, формой или размером кнопки ”Дать согласие“.

Оператору, обрабатывающему файлы cookie, необходимо разместить на сайте Политику в отношении обработки файлов cookie на уровне не ниже второго или на главной странице сайта, или на странице, доступной с главной.

Возможным вариантом может быть размещение этого документа в футере сайта, чтобы субъект персональных данных на любой странице мог его найти.

Какие обязательные меры должен принять оператор (уполномоченное лицо) по защите персональных данных?

	Юридические лица	**Индивидуальные предприниматели**	**Иные физические лица, осуществляющие индивидуальную предпринимательскую деятельность**
Назначение лица, ответственного за внутренний контроль	+	-	-
Издание политики в отношении обработки персональных данных	+	+	-
Ознакомление работников с положениями законодательства о персональных данных и соответствующими внутренними документами оператора, определяющими такую обработку, обучение персонала	+	+ *** требование обязательно только в случае наличия наемных работников**	+ *** требование обязательно только в случае наличия наемных работников**
Установление порядка доступа к персональным данным	+	+	+

Осуществление технической и криптографической защиты персональных данных	+	+	+

Нужно ли уведомлять Центр о начале обработки персональных данных (привлечении уполномоченного лица)?

Уведомление уполномоченного органа по защите прав субъектов персональных данных о начале обработки персональных данных и (или) привлечении уполномоченных лиц не требуется.

Что такое Реестр операторов персональных данных и какие сведения в него включаются?

В Реестр операторов персональных данных включаются сведения об информационных ресурсах (системах), в которых обрабатываются персональные данные.

Указом Президента Республики Беларусь от 28 октября 2021 г. № 422 ”О мерах по совершенствованию защиты персональных данных“ установлена обязанность операторов вносить в Реестр операторов персональных данных сведения об информационных ресурсах (системах), содержащих персональные данные по соответствующим критериям, установленным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 1 июня 2022 г. № 94 ”О государственном информационном ресурсе ”Реестр операторов персональных данных“.

В Реестр операторов персональных данных подлежат внесению сведения об информационных ресурсах (системах), посредством которых осуществляется:

трансграничная передача специальных персональных данных, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных (за исключением случаев, предусмотренных абзацами пятым – седьмым пункта 1 статьи 9 Закона);

обработка биометрических и (или) генетических персональных данных;

обработка персональных данных более 100 тыс. физических лиц;

обработка персональных данных более 10 тыс. физических лиц, не достигших возраста шестнадцати лет.

Подробнее с информацией о Реестре операторов персональных данных можно ознакомиться на сайте Центра ((https://cpd.by/zachita-personalnyh-dannyh/operatoru/reestr-operatorov-personalnih-dannih/).

Что такое трансграничная передача персональных данных?

Если в ходе обработки персональных данных они передаются на территорию иностранного государства, то происходит трансграничная передача персональных данных.

Например, трансграничная передача персональных данных имеет место при:

хранении сведений о клиентах на серверах, размещенных за пределами Республики Беларусь (Google Drive, Dropbox, iCloud, Яндекс Диск и др.);

передаче персональных данных партнеру, находящемуся в иностранном государстве;

использовании для передачи персональных данных иностранных мессенджеров и электронной почты вне белорусской доменной зоны (Viber, Telegram, WhatsApp, Gmail и др.);

публикации фотоизображений и иных персональных данных клиентов в социальных сетях (Instagram, TikTok и др.);

предоставлении услуги бронирования отелей, других мест проживания и посещения для своих клиентов на время их пребывания в иностранном государстве;

предоставлении сведений о бывших работниках по запросу иностранной организации;

использовании CRM (за исключением случаев использования субъектами малого предпринимательства коробочной версии, которая представляет собой локальную установку системы на сервере оператора);

предоставлении персональных данных гражданина для оказания медицинской помощи за рубежом;

осуществлении онлайн-записи через сервисы YClient, Telegram-бот и иные, через директ социальной сети.

Необходимо ли получать разрешение Центра или иных органов для трансграничной передачи персональных данных?

Если персональные данные передаются на территорию государств, где обеспечивается надлежащий уровень защиты прав субъектов персональных данных, то соблюдаются общие положения обработки персональных данных без получения дополнительных разрешений.

Если персональные данные передаются на территорию государств, не обеспечивающих надлежащий уровень защиты прав субъектов персональных данных, то для такой передачи необходимо самостоятельное правовое основание, предусмотренное статьей 9 Закона.

Одним из таковых выступает разрешение уполномоченного органа по защите прав субъектов персональных данных (абзац восьмой

пункта 1 статьи 9 Закона), порядок получения которого регламентируется приказом Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 14 ”О трансграничной передаче персональных данных“.

При этом без разрешения трансграничная передача персональных данных допускается, например, в случаях, когда:

дано согласие субъекта персональных данных при условии, что субъект персональных данных проинформирован о рисках, возникающих в связи с отсутствием надлежащего уровня их защиты;

персональные данные получены на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором;

персональные данные могут быть получены любым лицом посредством направления запроса в случаях и порядке, предусмотренных законодательством;

такая передача необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;

обработка персональных данных осуществляется в рамках исполнения международных договоров Республики Беларусь;

такая передача осуществляется органом финансового мониторинга в целях принятия мер по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения в соответствии с законодательством.

Можно ли оператору передавать персональные данные на хранение за границу (например, иностранному уполномоченному лицу для организации хранения клиентской базы)?

Законодательство о персональных данных не содержит ограничений в части возможности привлечения иностранных уполномоченных лиц и использования операторами иностранных сервисов в их деятельности.

При этом при поручении обработки персональных данных уполномоченному лицу – резиденту иностранного государства оператор должен убедиться в том, что этим лицом приняты и соблюдаются меры по обеспечению защиты персональных данных, включая осуществление внутреннего контроля за обработкой персональных данных, издание документов, определяющих политику в отношении обработки персональных данных, техническую и криптологическую защиту

информации, эквивалентные мерам, предусмотренным белорусским законодательством.

Кроме того, при осуществлении трансграничной передачи персональных данных организациям необходимо учитывать положения пункта 2 Указа Президента Республики Беларусь от 1 февраля 2010 г. № 60 ”О мерах по совершенствованию использования национального сегмента сети Интернет“, которым устанавливается обязанность юридических лиц, их филиалов и представительств, созданных в соответствии с законодательством Республики Беларусь, с местонахождением в Республике Беларусь, а также индивидуальных предпринимателей, зарегистрированных в Республике Беларусь осуществлять деятельность по реализации товаров, выполнению работ, оказанию услуг на территории Республике Беларусь с использованием информационных сетей, систем и ресурсов национального сегмента сети Интернет, размещенных на территории Республики Беларусь и зарегистрированных в установленном порядке.

Какая ответственность предусмотрена за нарушение законодательства о персональных данных?

За нарушение законодательства о персональных данных предусмотрена:

1. дисциплинарная ответственность (пункт 10 части первой статьи 47 Трудового кодекса Республики Беларусь);
2. административная ответственность (статья 23.7 Кодекса Республики Беларусь об административных правонарушениях);
3. уголовная ответственность (статья 203^1, 203^2 Уголовного кодекса Республики Беларусь);
4. гражданско-правовая ответственность (пункт 2 статьи 19 Закона предусматривает возмещение морального вреда, имущественного вреда и понесенных субъектом персональных данных убытков).

Важно также помнить о репутационных рисках, которые влечет недобросовестная обработка персональных данных граждан.

Где взять формы документов и дополнительную информацию по вопросам защиты персональных данных?

На сайте Центра (https://cpd.by/) в разделе ”Правовая основа“ – ”Методологические документы“ – ”Портфель оператора“ (https://cpd.by/pravovaya-osnova/metodologicheskie-dokumenty-test/portfel-operatora/) размещены примерные формы (образцы) документов, необходимых операторам (уполномоченным лицам) для организации работы по надлежащей реализации Закона, в том числе:

Форма согласия на обработку персональных данных;

Должностная инструкция специалисту по внутреннему контролю;

Примерная политика в отношении обработки персональных данных;

Примерная политика в отношении обработки персональных данных в процессе трудовой деятельности;

Примерная политика в отношении обработки файлов cookie;

Примерная политика видеонаблюдения;

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

С дополнительной информацией (разъяснениями, рекомендациями, алгоритмом приведения деятельности операторов, уполномоченных лиц в соответствие с требованиями Закона и др.) можно ознакомиться в разделе ”Правовая основа“ – ”Методологические документы“ (https://cpd.by/pravovaya-osnova/metodologicheskie-dokumenty-test/).

На сайте Центра также размещен Постатейный комментарий к Закону (https://cpd.by/pravovaya-osnova/metodologicheskiye-dokumenty-rekomendatsii/postatejnyj-kommentarij-k-zakonu-respubliki-belarus-o-zashhite-personalnyh-dannyh/).

Кроме того, дополнительная информация по вопросам защиты персональных данных публикуется Центром в следующих социальных сетях:

https://www.instagram.com/cpd_by/;

https://t.me/cpd_by;

https://www.youtube.com/channel/UCZ7YB80BA-TvXW4sqpqV6mg;

https://by.linkedin.com/company/cpd-by;

https://vm.tiktok.com/ZMBJEfx8F/;

https://www.facebook.com/share/1BdofZfYhN/.