



**ЧЕК-ЛИСТ
ПОДГОТОВКИ КОМПАНИИ
К ВСТУПЛЕНИЮ В СИЛУ ЗАКОНА
«О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ»**

REVERA

50+

адвокатов и юристов

REVERA – самая крупная
юридическая компания Беларуси

CHAMBERS
AND PARTNERS

THE
LEGAL
500

IFLR1000

По мнению экспертов – REVERA один
из лидеров на рынке юридических услуг

20+

лет на рынке

Опыт работы на юридическом
рынке Беларуси

14

направлений

Работаем в 14 направлениях и 8
отраслях, имея узкую экспертизу
в различных областях права и
бизнеса

Алёна Поторская
руководитель проектов
в сфере конфиденциальности
и защиты персональных данных
anp@revera.by



Уважаемые коллеги!

Как вы знаете, 28 октября 2021 года был принят Указ «О дополнительных мерах по защите персональных данных». И с 15 ноября 2021 года Закон «О защите персональных данных» вступает в силу. Уже создан контролирующий орган НЦЗПД, разработаны процедуры, определена ответственность.

Команда REVERA разработала для вас Чек-лист подготовки вашей компании к вступлению в силу Закона «О защите персональных данных».

Для кого?

Чек-лист предназначен сотруднику компании, который будет заниматься приведением процессов работы с персональными данными в соответствие с Законом (юрист, директор, бухгалтер и иные должности).

Для чего?

Чек-лист содержит пошаговую инструкцию, что необходимо сделать в компании для имплементации Закона и разработан для того, чтобы помочь вам в этом.

Что в итоге?

Результатом работы с этим документом у компании будет полное понимание того, с какими данными она работает, в каких целях и на каких основаниях. А также будет понятен перечень документов и мер, которые нужно разработать и внедрить.

Команда юристов REVERA сможет помочь вам разобраться в нюансах нового Закона, а также решить все сопутствующие вопросы, в том числе разработка документов, шаблонов документов, внутренних политик и регламентов, организация обучения для сотрудников, разрешение возможных споров.

Команда REVERA

ЧЕК-ЛИСТ

ПОДГОТОВКИ КОМПАНИИ К ВСТУПЛЕНИЮ В СИЛУ ЗАКОНА «О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ»

АКТУАЛЕН НА МОМЕНТ 5 НОЯБРЯ 2021 ГОДА

1 Назначить ответственное лицо

Документы:

- приказ о назначении
- должностная инструкция/дополнения в должностную инструкцию (если это не отдельная должность)

2 Определить, в каких «точках» компания работает с персональными данными (сайты, приложения, HR (кандидаты и работники), договоры с контрагентами, программы лояльности и прочее)

3 Определить цель каждой обработки и убедиться, что все запрашиваемые персональные данные необходимы для данных целей — излишние данные исключить (не запрашивать)

4 Определить надлежащее правовое основание для каждой обработки (согласие, трудовые отношения, договор, обработка общедоступных данных, требования законодательства и иное)

Документы по п. 2, 3, 4: реестр обработки персональных данных

5 Разработать политику обработки персональных данных в компании и сопутствующие документы, необходимые для систематизации процессов

Документы:

- положение об обработке ПД (ЛПА)
- регламент реагирования на запросы субъектов ПД
- типовые формы заявлений субъектов о реализации их прав
- типовые формы ответов на заявления субъектов о реализации их прав (или отказов в реализации)
- журнал учета заявлений субъектов ПД

- 6** Разработать и поддерживать в актуальном состоянии:
- перечень информационных ресурсов (систем), содержащих персональные данные, собственниками (владельцами) которых является компания
 - категории персональных данных, подлежащих включению в такие ресурсы (системы): общедоступные; специальные (кроме биометрических и генетических); биометрические и генетические; персональные данные, не являющиеся общедоступными или специальными
 - перечень уполномоченных лиц, если обработка персональных данных осуществляется такими лицами
 - срок хранения обрабатываемых персональных данных

Документы:

- перечни, перечисленные выше

- 7** Провести разграничение доступа к персональным данным

Документы и шаги:

- положение о порядке доступа к персональным данным
- принять реальные технические меры, которые позволят предотвратить несанкционированный доступ

- 8** Ознакомить работников с документами из п. 5 и п. 6, законодательством о защите персональных данных, провести инструктаж по работе с персональными данными. При этом, необходимо организовывать не реже одного 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

Документы:

- журнал проведения инструктажа;
- иные документы, подтверждающие прохождение обучения

- 9** Разработать политику обработки персональных данных для сайта и (или) приложения

REVERA рекомендует иметь отдельные документы для сайтов и (или) приложений (с информацией для клиентов) и внутренний локальный правовой акт (где будут содержаться правила для работников (п. 5 и п. 6 выше)). При этом, политика обработки данных для сайтов и (или) приложений должна быть написана простым и понятным языком, поскольку пишется для пользователей

Документ: политика обработки персональных данных

10

По результатам проведённой работы, внести изменения в заключённые/заключаемые документы

Пример:

- разработать текст согласия для кандидатов и следить за его получением от кандидатов перед началом обработки их персональных данных
- исключить согласие на обработку персональных данных из трудового договора, поскольку в такой форме оно является вынужденным
- разработать текст отдельного согласия с работниками и получить такое согласие от каждого работника
- отредактировать анкету для участия в программе лояльности (убрать излишние данные, добавить форму для запроса согласия в надлежащей форме)
- изменить форму запроса данных на сайте и (или) в приложениях (убрать излишние данные, добавить форму для запроса согласия в надлежащей форме)

При этом, важно следить за целями обработки персональных данных. Если цели изменились со временем — необходимо получить новое согласие

11

Оформить поручения на обработку персональных данных с уполномоченными лицами

12

Проработать технические вопросы реагирования на запросы субъектов персональных данных (обеспечить возможность отзыва согласия, удаления данных и так далее)

13

Принимать меры по технической и криптографической защите информационных систем