



ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ.

Пошаговый алгоритм организационных действий по работе с персональными данными сотрудников

КРАТКИЙ ОБЗОР РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В НОВОМ ЗАКОНЕ



История создания

Цель

Основные принципы



Что имеем сегодня

Указ Президента Республики Беларусь от 28.10.2021 № 422
«О мерах по совершенствованию защиты персональных данных»

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12.11.2021 № 194
«Об обучении по вопросам защиты персональных данных»

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12.11.2021 № 195
«О технической и криптографической защите персональных данных»

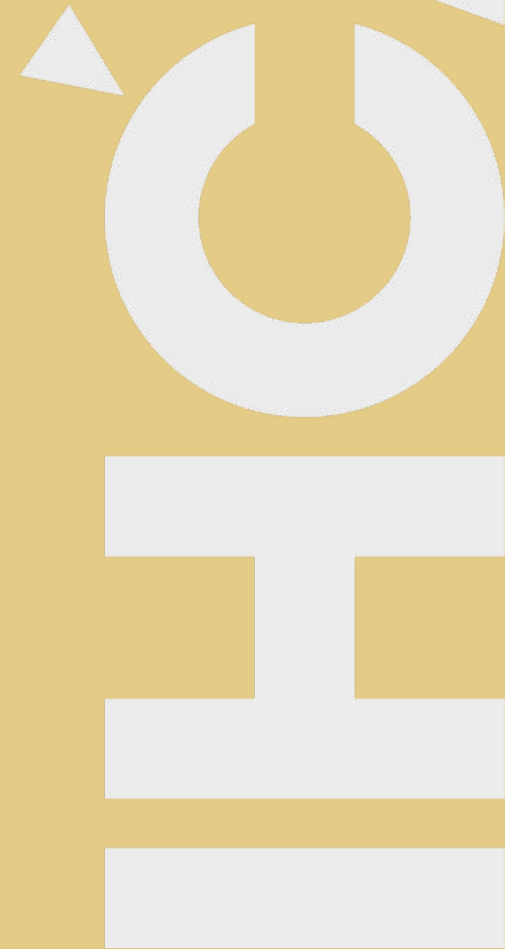
ПРИКАЗ НАЦИОНАЛЬНОГО ЦЕНТРА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РЕСПУБЛИКИ БЕЛАРУСЬ
15 ноября 2021 г. № 14
«О трансграничной передаче персональных данных»

ПРИКАЗ НАЦИОНАЛЬНОГО ЦЕНТРА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РЕСПУБЛИКИ БЕЛАРУСЬ
15 ноября 2021 г. № 13
«Об уведомлении о нарушениях систем защиты персональных данных»

Рекомендации по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных



ОСНОВНЫЕ ТЕРМИНЫ ЗАКОНА И СУБЪЕКТЫ ОТНОШЕНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ



16 терминов

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ – любое **действие** или совокупность действий, совершаемые с персональными данными:

- сбор
- систематизация,
- хранение,
- изменение,
- использование,
- обезличивание,
- блокирование,
- распространение,
- предоставление,
- удаление

Оператор

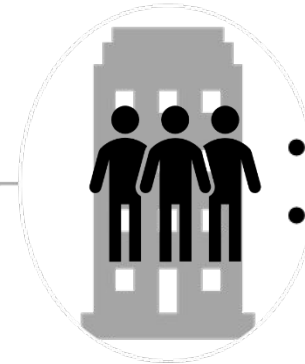


Ответственный за осуществление внутреннего контроля за обработкой ПД

Работник оператора, осуществляющий обработку персональных данных

Уполномоченное лицо

Субъект ПД



- внешний
- внутренний



Оператор



КТО?

- государственный орган
- юридическое лицо Республики Беларусь (**ВАША КОМПАНИЯ**)
- иная организация
- физическое лицо
- индивидуальный предприниматель

ЧТО?

самостоятельно или совместно с иными указанными лицами:
организующие и (или) осуществляющие обработку персональных данных



Субъект ПД



КТО?

физическое лицо, в отношении которого осуществляется обработка персональных данных

ЧТО?

биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации

- отпечатки пальцев рук, ладоней,
- радужная оболочка глаза,
- характеристики лица и его изображение и другое

генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека:

- содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца

специальные персональные данные:

- расовая либо национальная принадлежность,
- политические взгляды,
- членство в профессиональных союзах,
- религиозные или другие убеждения,
- здоровье или половая жизнь,
- привлечение к административной или уголовной ответственности



Ответственный за осуществление
внутреннего контроля за обработкой
ПД



КТО?

- структурное подразделение
- лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных

Работник, осуществляющий обработку
ПД



КТО?

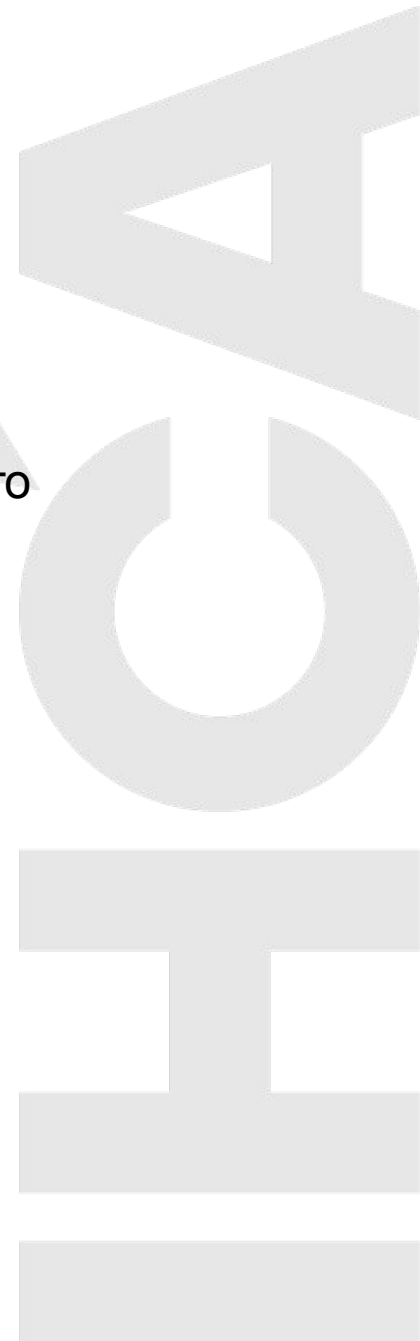
- работник любого структурное подразделения

Работник, имеющий доступ к ПД

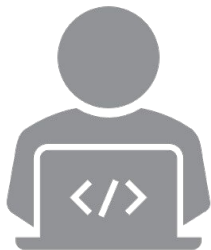


КТО?

- любой работник оператора



Уполномоченное лицо



КТО?

- государственный орган
- юридическое лицо Республики Беларусь
- иная организация
- физическое лицо

ЧТО?

осуществляют обработку персональных данных от имени оператора или в его интересах в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором



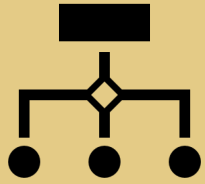
Уполномоченное лицо

Внешний

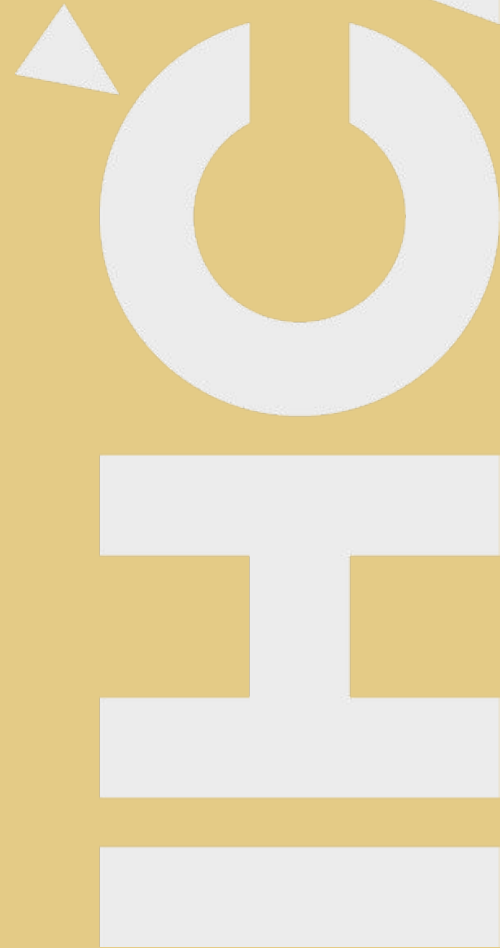
аутсорсер

компания по
сопровождению
ПО



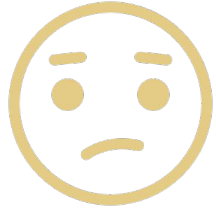


АЛГОРИТМ ДЕЙСТВИЙ





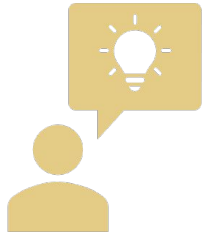
1



Не паникуем!
Время все расставит на свои места



2



Максимально информируем всех в компании о вступлении в силу с 15.11.2021 Закона от 07.05.2021 № 99-З «О защите персональных данных»

3



Решаем, какая служба (работник) будет координировать и организовывать работу, связанную с вступлением в силу Закона

3.1. Документы



- приказ о создании рабочей группы;
- план мероприятий по защите персональных данных

3.2. Важно

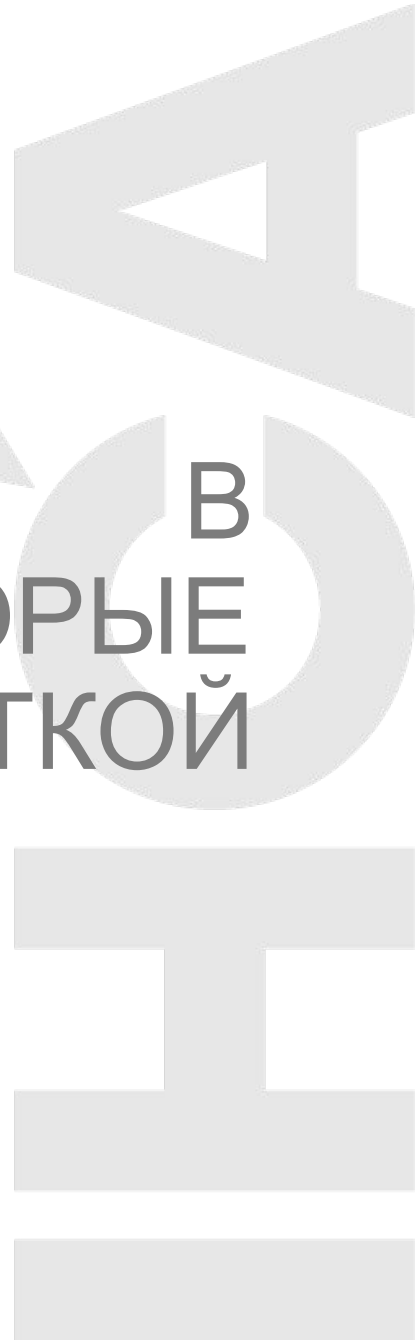


! Не забываем, что это **очень большой дополнительный объем работы**, не предусмотренный функционалом на текущий момент

4



ЗАПРАШИВАЕМ ИНФОРМАЦИЮ В
ПОДРАЗДЕЛЕНИЯХ, КОТОРЫЕ
СВЯЗАНЫ С ОБРАБОТКОЙ
ПЕРСОНАЛЬНЫХ ДАННЫХ



4.1. Документы



1. Составляем перечень подразделений

2. Направляем руководителям просьбу предоставить информацию о процедурах, при осуществлении которых могут использоваться персональные данные, непосредственно какие данные используются и кто имеет доступ к их обработке (за исключением ПД, где не требуется получение согласия работника)

3. Обобщаем полученную информацию для:

- определения процедур, требующих получения согласия субъекта персональных данных;
- определения целей, для которых могут использоваться персональные данные;
- определения круга лиц, непосредственно осуществляющих обработку персональных данных;
- оптимизации работы, связанной с получением и обработкой персональных данных

5



НАЗНАЧАЕМ СТРУКТУРНОЕ
ПОДРАЗДЕЛЕНИЕ ИЛИ ЛИЦО,
ОТВЕТСТВЕННОЕ ЗА
ОСУЩЕСТВЛЕНИЕ ВНУТРЕННЕГО
КОНТРОЛЯ ЗА ОБРАБОТКОЙ
ПЕРСОНАЛЬНЫХ ДАННЫХ



5.1. Документы



Ответственный за
осуществление
внутреннего контроля за
обработкой ПД

Лицо

Новый сотрудник

Действующий сотрудник

приказ

должностная инструкция

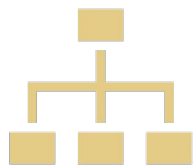
уведомление об изменении
существенных условий
труда

дополнительное
соглашение к
контракту/трудовому
договору

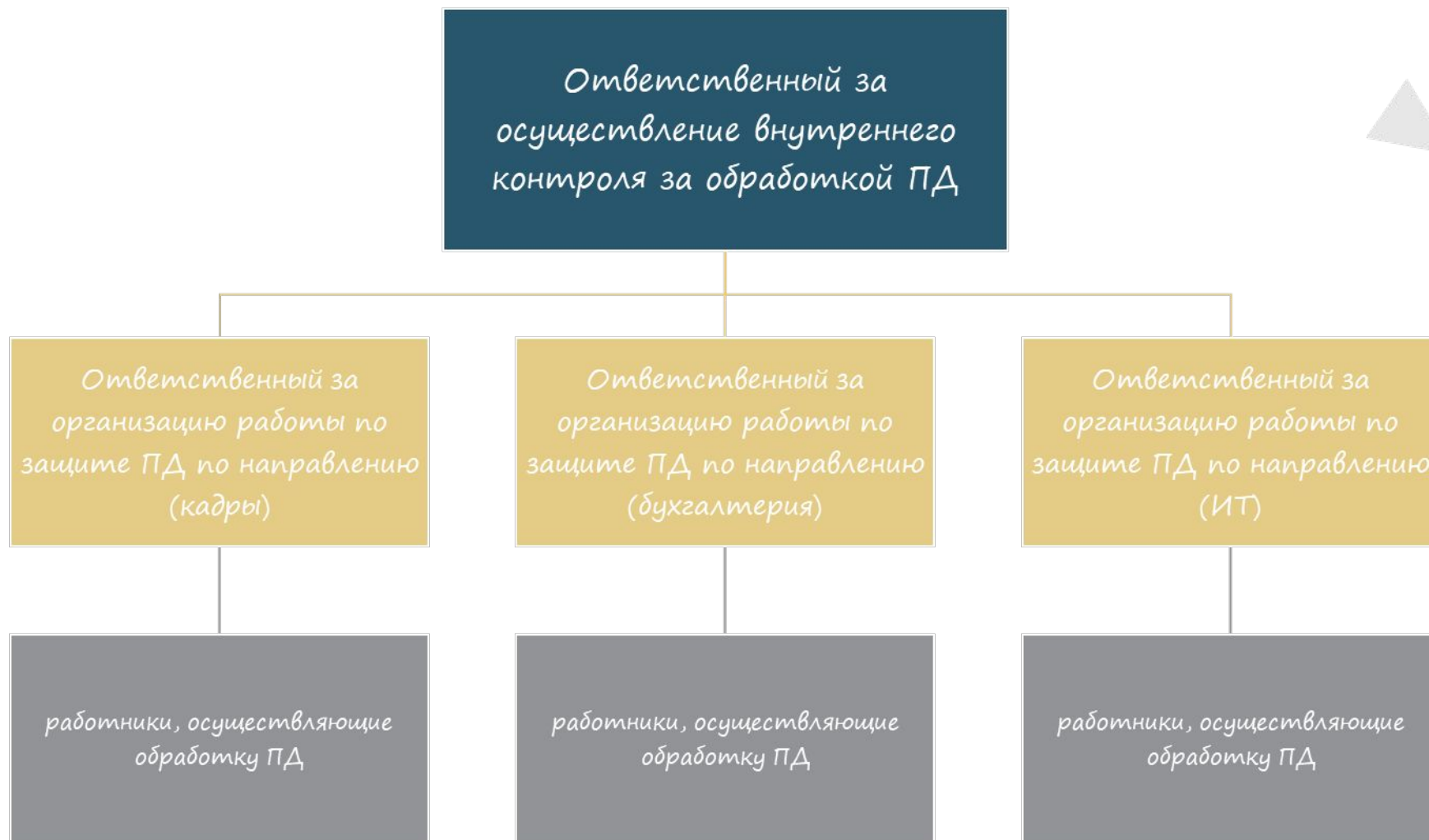
дополнение в
должностную
инструкцию

! Не забыть в приказе определить лицо, осуществляющее данные функции в период отсутствия первоначально назначенного

5.1. Документы



5.2. Как выстроить взаимодействие





СОСТАВЛЯЕМ ПРИМЕРНЫЙ
ПЕРЕЧЕНЬ ОРГАНИЗАЦИОННО-
РАСПОРЯДИТЕЛЬНЫХ
ДОКУМЕНТОВ,
РЕГЛАМЕНТИРУЮЩИХ ПОРЯДОК
РАБОТЫ С ПЕРСОНАЛЬНЫМИ
ДААННЫМИ

6.1. Документы



основные ЛПА (политика, положения, регламенты);

ЛПА, регламентирующие деятельность отдельных лиц (инструкции (например, о порядке доступа в помещение, где ведется обработка персональных данных));

приказы (назначение комиссий, мест хранения, утверждение перечней и т.д.);

документы, фиксирующие определенные факты или события (протоколы, акты, заключения);

формы документов (уведомления, обязательства и пр.)





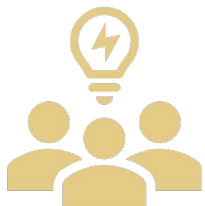
7



ПРИСТУПАЕМ К РАЗРАБОТКЕ
РЕГЛАМЕНТИРУЮЩИХ ПОРЯДОК
ПЕРСОНАЛЬНЫМИ ДАННЫМИ

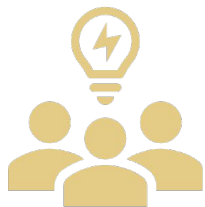
ДОКУМЕНТОВ,
РАБОТЫ С

A large, light gray watermark logo is positioned on the right side of the slide. It consists of a stylized letter 'A' at the top, a circular symbol with a central dot in the middle, and a vertical bar with horizontal segments at the bottom, resembling a stylized 'E' or a similar symbol.



ПРОВОДИМ ОБУЧЕНИЕ И РАБОТУ С
ЛИЦАМИ, НЕПОСРЕДСТВЕННО
ОСУЩЕСТВЛЯЮЩИМИ ОБРАБОТКУ
ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Документы



разъяснение норм Закона и порядка доступа к информации

уведомление об ответственности за нарушение законодательства о защите персональных данных

включение в трудовые договоры и должностные инструкции соответствующих обязанностей и ответственности

подписание обязательств о неразглашении



ИНФОРМИРУЕМ СУБЪЕКТОВ
ПЕРСОНАЛЬНЫХ ДАННЫХ
КОМПАНИИ О ПРОВОДИМОЙ
РАБОТЕ ПО ЗАЩИТЕ ИХ
ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Документы

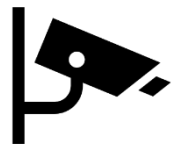


- уведомление субъекта персональных данных (работника) о предоставлении ему информации до получения его согласия на обработку персональных данных;
- уведомление СПД о разъяснении его прав, связанных с обработкой персональных данных, до получения его согласия на обработку персональных данных;
- получение письменных согласий от СПД на обработку их персональных данных (за исключением случаев, предусмотренных Законом)

▶ Не забудьте учесть!



АУДИО



ВИДЕО



ФОТО



10



ПРОДУМЫВАЕМ, КАК БУДЕТ
ОСУЩЕСТВЛЯТЬСЯ ФИЗИЧЕСКАЯ И
ТЕХНИЧЕСКАЯ ЗАЩИТА
ПЕРСОНАЛЬНЫХ ДАННЫХ

- планирование бюджета;
- оборудование помещений;
- программное обеспечение и пр.



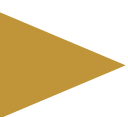


ПРИМЕРНЫЙ ПЕРЕЧЕНЬ
ПРОЦЕДУР И ДЕЙСТВИЙ, ГДЕ
МОГУТ БЫТЬ ЗАДЕЙСТВОВАНЫ
ПЕРСОНАЛЬНЫЕ ДАННЫЕ
РАБОТНИКОВ



ПРИМЕР МАТРИЦЫ КОМПАНИИ ПО СИСТЕМАТИЗАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

Подразделение/ направление деятельности	Процедура	Действие	Перечень данных	Способ размещения	Должность лица, осуществляю щего обработку	ФИО
1. КАДРЫ	1.1. Прием на работу	1.1.1. Карточка формы Т-2	идентификационный номер; фамилия, собственное имя, отчество (если таковое имеется); пол; число, месяц, год рождения; место рождения; цифровой фотопортрет; данные о гражданстве (подданстве); данные о регистрации по месту жительства и (или) месту пребывания; семейном положении, супруге, ребенке (детях) физлица; данные о высшем образовании, ученой степени, ученом звании; данные об инвалидности	На бумажном носителе	специалист по кадрам	Иванова Петрова Сидорова
		1.1.2. Автобиография	Дополнительно: данные о родителях, опекунах, супруге, ребенке (детях) с указанием даты рождения; сведения о привлечении к административной и уголовной ответственности	На бумажном носителе	специалист по кадрам	Иванова Петрова Сидорова
		1.1.3. Анкета компании	Дополнительно: вероисповедание а также данные о родителях, ответственности	В электронном виде в АСУ «Кадры»	Начальник отдела кадров	Филонова



ПОДРАЗДЕЛЕНИЯ, РАБОТАЮЩИЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКОВ

Служба безопасности

Кадры

Служба персонала

Бухгалтерия

Архив

Юридическая служба

Охрана труда

Секретари

ИТ

PR

Руководитель и линейные руководители



Форма получения согласия работником

В письменной форме.

В виде электронного документа.

Посредством проставления физлицом соответствующей отметки на интернет-ресурсе.

Через указание физлицом определенной информации после получения СМС-сообщения или письма по электронной почте.





ОБУЧЕНИЕ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ





Чья обязанность?

Оператора

Когда и кого обучать?

1 раз в 5 лет:

1. Ответственных за осуществление внутреннего контроля за обработкой персональных данных
2. Лиц, непосредственно осуществляющих обработку персональных данных

1 раз в 3 года:

3. Работники и (или) иные лица, в обязанности которых входит обеспечение информационной безопасности



Где обучать?

1. Ответственных за осуществление внутреннего контроля за обработкой персональных данных у операторов, определенных ОАЦ,

в банках и небанковских кредитно-финансовых организациях;

в страховых организациях;

у операторов электросвязи (за исключением индивидуальных предпринимателей);

в республиканской и территориальных организациях по государственной регистрации недвижимого имущества, прав на него и сделок с ним;

в Белорусской нотариальной палате, областных (Минской городской) нотариальных палатах;

в риэлтерских организациях;

в организациях здравоохранения;

в местных исполнительных и распорядительных органах (за исключением сельских (поселковых) исполнительных комитетов), их структурных подразделениях с правами юридического лица;

у операторов (уполномоченных лиц), организующих и (или) осуществляющих обработку персональных данных не менее 10 тыс. физических лиц, за исключением персональных данных работников этих операторов (уполномоченных лиц) в процессе осуществления трудовой (служебной) деятельности

в НЦЗПД

по образовательной программе повышения квалификации руководящих работников и специалистов

ДО 15.12. В НЦЗПД ПОДАТЬ СВЕДЕНИЯ!



Где обучать?

2. Работники и (или) иные лиц, в обязанности которых входит обеспечение информационной безопасности

в организациях, которые являются собственниками (владельцами) информационных систем и владельцами критически важных объектов информатизации, а также организации, осуществляющие лицензируемую деятельность по технической и (или) криптографической защите информации

в НЦЗПД

по образовательной программе повышения квалификации руководящих работников и специалистов по вопросам технической и (или) криптографической защиты информации

**ДО 15.11. В НЦЗПД ПОДАВАТЬ СВЕДЕНИЯ!
В ЭТОМ ГОДУ ДО 15.12.**

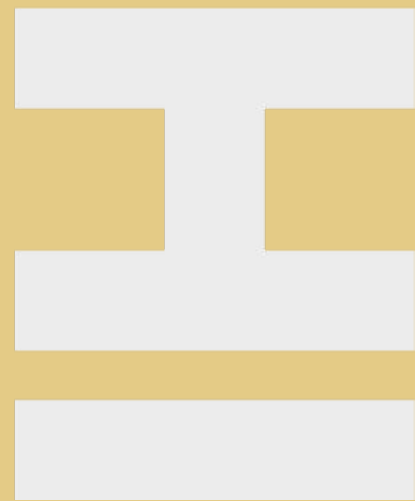


3. ВСЕ ОСТАЛЬНЫЕ!

- 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)



РЕЕСТР ПЕРСОНАЛЬНЫХ ДАННЫХ



КТО ВЕДЕТ?



Республиканский – НЦЗПД
РЕЕСТР ОПЕРАТОРОВ
ПЕРСОНАЛЬНЫХ ДАННЫХ
Срок определения перечня сведений
для внесения в реестр - 01.08.2022



Оператор – ваша компания
Не обязателен, сроки не
установлены

ЧТО ВКЛЮЧАЕТ?

перечень информационных ресурсов (систем), содержащих персональные данные, собственниками (владельцами) которых они являются;

категории персональных данных, подлежащих включению в такие ресурсы (системы):

- общедоступные персональные данные;
- специальные персональные данные (кроме биометрических и генетических персональных данных);
- биометрические и генетические персональные данные;
- персональные данные, не являющиеся общедоступными или специальными;

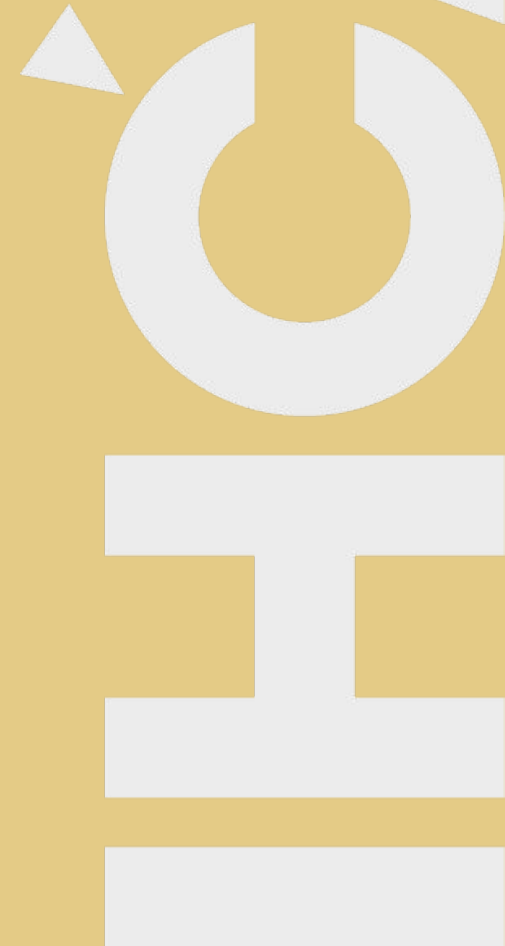
перечень уполномоченных лиц, если обработка персональных данных осуществляется уполномоченными лицами;

срок хранения обрабатываемых персональных данных.

Должна быть обеспечена актуализация соответствующих сведений!



ОТВЕТСТВЕННОСТЬ ЗА
НАРУШЕНИЕ
ЗАКОНОДАТЕЛЬСТВА,
РЕГЛАМЕНТИРУЮЩЕГО ВОПРОСЫ
ИСПОЛЬЗОВАНИЯ
ПЕРСОНАЛЬНЫХ ДАННЫХ



дисциплинарная

- п. 10 ч. 1 ст. 47 ТК трудовой договор с некоторыми категориями работников может быть **прекращен** в случаях нарушения работником порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных

административная

- Ст.23.7. Нарушение законодательства о защите персональных данных
 - Умышленные незаконные сбор, обработка, хранение или предоставление персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных, – влекут наложение штрафа в размере до **50 базовых** величин.
 - Деяния, предусмотренные частью 1 настоящей статьи, совершенные лицом, которому персональные данные известны **в связи с его профессиональной или служебной деятельностью**, – влекут наложение штрафа в размере от **4 до 100 базовых** величин.
 - Умышленное незаконное распространение персональных данных физических лиц – влечет наложение штрафа в размере **до 200 базовых величин**.
 - Несоблюдение мер обеспечения защиты персональных данных физических лиц – влечет наложение штрафа в размере от двух до десяти базовых величин, на индивидуального предпринимателя – от десяти до двадцати

уголовная

- [ст. 203¹](#) «Незаконные действия в отношении информации о частной жизни и персональных данных»: общественные работы, или штраф, или арест, или **ограничение свободы на срок до 5 лет** или лишение свободы на тот же срок со штрафом;
- [ст. 203²](#) «Несоблюдение мер обеспечения защиты персональных данных»: несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку персональных данных, повлекшее по неосторожности их распространение и причинение тяжких последствий, наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до 1 года, или арестом, или ограничением свободы на срок до 2 лет, или **лишением свободы на срок до 1 года**;