

Приложение №4

Общество с ограниченной
ответственностью «Караван XXI век»
(ООО «Караван XXI век»)



ПОЛОЖЕНИЕ

15.11.2021 №4

Минский район

О порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные

ГЛАВА 1 ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение устанавливает применяемые в обществе с ограниченной ответственностью «Караван XXI век» (далее - Организация) способы обеспечения безопасности при обработке персональных данных, которыми являются любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных.

2. Настоящее Положение разработано на основании Конституции Республики Беларусь; Закона Республики Беларусь от 07.05.2021 №99-З «О защите персональных данных»; Закона Республики Беларусь от 21.07.2008 №418-З «О регистре населения»; Закона Республики Беларусь от 10.11.2008 №455-З «Об информации, информатизации и защите информации» и иных нормативных правовых актов Республики Беларусь.

3. В соответствии с законодательством Республики Беларусь под персональными данными понимается любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая Организации в связи с трудовыми отношениями.

4. Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное для соблюдения должностными лицами Организации, допущенными к обработке персональных данных, иными получившими доступ к персональным данным лицами требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

5. Обеспечение конфиденциальности персональных данных не требуется в случае:

обезличивания персональных данных (действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных);

для общедоступных персональных данных (персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов).

6. Перечни персональных данных и ответственных за хранение и обработку персональных данных утверждается приказом директора Организации.

Обработка и хранение конфиденциальных данных лицами, не указанными в приказе, запрещается.

7. В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных Организация предоставляет должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований:

знакомит работника под подпись с требованиями Политики оператора в отношении обработки персональных данных ООО «Караван XXI век», с Положением об обработке и защите персональных данных ООО «Караван XXI век», с настоящим Положением о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные, с должностной инструкцией и иными локальными правовыми актами Организации в сфере обеспечения конфиденциальности и безопасности персональных данных;

представляет хранилища для документов, средства для доступа к информационным ресурсам (ключи, пароли и т. п.);

обучает правилам эксплуатации средств защиты информации;

проводит иные необходимые мероприятия.

8. Должностным лицам Организации, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных.

Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

9. Должностные лица Организации, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с исполнением своих трудовых обязанностей.

10. При прекращении выполнения трудовой функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении должностного лица в связи с исполнением

должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

11. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством Республики Беларусь, Политикой оператора в отношении обработки персональных данных ООО «Караван XXI век», Положением об обработке и защите персональных данных ООО «Караван XXI век», Положением о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные ООО «Караван XXI век», должностной инструкцией и иными локальными правовыми актами Организации в сфере обеспечения конфиденциальности и безопасности персональных данных

Передача персональных данных осуществляется ответственным за обработку персональных данных должностным лицом Организации на основании письменного или устного поручения руководителя структурного подразделения.

12. Передача сведений и документов, содержащих персональные данные, оформляется путем составления акта по установленной форме.

13. Должностное лицо, предоставившее персональные данные третьим лицам, направляет письменное уведомление субъекту персональных данных о факте передачи его данных третьим лицам.

14. Запрещается передача персональных данных по телефону, факсу, электронной почте, за исключением случаев, установленных законодательством и действующими в Организации локальными правовыми актами.

Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

15. Должностные лица Организации, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и (или) главному специалисту по информационной безопасности обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостатке носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

16. Должностные лица, осуществляющие обработку персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Республики Беларусь.

17. Отсутствие контроля со стороны Организации за надлежащим исполнением работником своих обязанностей в области обеспечения конфиденциальности и безопасности персональных данных не освобождает работника от таких обязанностей и предусмотренной законодательством Республики Беларусь ответственности.

ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

18. Обработка персональных данных, в том числе содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такая обработка осуществляется при непосредственном участии человека.

19. Руководитель структурного подразделения, осуществляющего обработку персональных данных без использования средств автоматизации:

определяет места хранения персональных данных (материальных носителей);

осуществляет контроль наличия в структурном подразделении условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;

информирует лиц, осуществляющих обработку персональных данных без использования средств автоматизации, о перечне обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

организует раздельное, то есть не допускающее смешение, хранение материальных носителей персональных данных (документов, дисков, дискет, USB флеш-накопителей, пр.), обработка которых осуществляется в различных целях.

20. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

21. При несовместимости целей обработки персональных данных руководитель структурного подразделения должен обеспечить раздельную обработку персональных данных.

22. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, должно производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

23. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе.

ГЛАВА 3

ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

24. Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники в компьютерной сети Организации (далее - КСО).

Безопасность персональных данных при их обработке в КСО обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в КСО информационные технологии.

Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Республики Беларусь требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в КСО, в установленном порядке проходят процедуру оценки соответствия.

25. Допуск лиц к обработке персональных данных с использованием средств автоматизации осуществляется на основании приказа директора Организации при наличии паролей доступа.

Работа с персональными данными, содержащимися в КСО, осуществляется в соответствии с «Регламентом действий пользователя», с которыми работник, в должностные обязанности которого входит обработка персональных данных, знакомится под подпись.

26. Работа с персональными данными в КСО должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

27. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, соответствующими требованиям «Регламента парольной защиты» ООО «Караван XXI век».

28. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернета, запрещается.

29. При обработке персональных данных в КСО пользователями должно быть обеспечено:

использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

30. При обработке персональных данных в КСО разработчиками и администраторами информационных систем должны обеспечиваться:

обучение лиц, использующих средства защиты информации, применяемые в КСО, правилам работы с ними;

учет лиц, допущенных к работе с персональными данными в КСО, прав и паролей доступа;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

описание системы защиты персональных данных.

31. Специфические требования по защите персональных данных в отдельных автоматизированных системах Организации определяются утвержденными в установленном порядке инструкциями по их использованию и эксплуатации.

ГЛАВА 4

ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ТВЕРДЫМИ КОПИЯМИ И ИХ УТИЛИЗАЦИИ

32. Все находящиеся на хранении и в обращении в Организации съемные носители (диски, дискеты, USB флеш-накопители, пр.), содержащие персональные данные, подлежат учету. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

33. Учет и выдачу съемных носителей персональных данных осуществляют работники Отдела инженерно-технической поддержки эксплуатации.

Работники Организации получают учетный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок.

При получении делаются соответствующие записи в журнале персонального учета съемных носителей персональных данных (далее - журнал учета), который ведется в Отделе инженерно-технической поддержки эксплуатации.

По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

34. При работе со съемными носителями, содержащими персональные данные, запрещается:

хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах либо оставлять их без присмотра или передавать на хранение другим лицам;

выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

35. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения Организации.

36. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено директору Организации.

На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета.

ГЛАВА 5 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

37. С настоящим Положением должны быть ознакомлены под подпись в Журнале учета допуска к обработке персональных данных все работники структурных подразделений Организации и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных работников Организации. Ответственный за инструктаж - администратор баз данных и информационных систем, в которых обрабатываются персональные данные.