

Приложение 3
к Политике оператора в отношении
обработки персональных данных

Закрытое акционерное общество
"Уайт Бёрд"

ПОЛОЖЕНИЕ
23.07.2024 №

г. Минск

О ПОРЯДКЕ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ
ПРИ ОБРАБОТКЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ
ПЕРСОНАЛЬНЫЕ ДАННЫЕ

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение устанавливает применяемые в Закрытом акционерном обществе "Уайт Бёрд" (далее – Общество) способы обеспечения безопасности при обработке персональных данных, которыми является 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:

2.1. Конституции;

2.2. Трудового кодекса;

2.3. Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981;

2.4. Хартии Европейского союза об основных правах от 12.12.2007;

2.5. Закона от 07.05.2021 № 99-3 "О защите персональных данных" (далее – Закон № 99-3);

2.6. Закона от 21.07.2008 № 418-3 "О регистре населения";

2.7. Закона от 10.11.2008 № 455-3 "Об информации, информатизации и защите информации";

2.8. Закона от 28.05.2021 № 114-3 "Об изменении законов по вопросам трудовых отношений";

2.9. иных НПА Республики Беларусь.

3. В соответствии с законодательством Республики Беларусь под персональными данными понимается любая информация, относящаяся к идентифицированному физлицу или физлицу, 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 Обществу в связи с трудовыми отношениями.

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

5. Обеспечение конфиденциальности персональных данных не требуется в случае:

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

5.2. 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 утверждаются приказом директора Общества.

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

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

7.1. знакомит работника под роспись с требованиями Политики оператора в отношении обработки персональных данных ЗАО "Уайт Бёрд", включая имеющиеся к ней приложения, с должностной инструкцией и иными локальными правовыми актами Общества в сфере обеспечения конфиденциальности и безопасности персональных данных;

7.2. представляет хранилища (в том числе облачные) для документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.);

7.3. проводит иные необходимые мероприятия.

8. Должностным лицам Общества, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью.

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



М.А. Шабанов

23.07.2024

10. Должностные лица Общества, работающие с персональными данными, обязаны при прекращении выполнения трудовой функции, связанной с обработкой персональных данных, исключить доступ ко всем носителям информации, содержащим персональные данные (оригиналам и копиям документов, машинным и бумажным носителям и пр.), которые находились в распоряжении должностного лица в связи с выполнением должностных обязанностей.

11. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством Республики Беларусь, Политикой оператора в отношении обработки персональных данных ЗАО "Уайт Бёрд", включая имеющиеся к ней приложения, должностной инструкцией и иными локальными правовыми актами Общества в сфере обеспечения конфиденциальности и безопасности персональных данных.

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

13. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими в Обществе 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.

14. Должностные лица Общества, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и (или) лицу, ответственному за информационную безопасность обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостаче 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.

15. 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.

16. Отсутствие контроля со стороны Общества 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.

ГЛАВА 2

ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

17. 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.

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

18.1. определяет места хранения персональных данных (материальных носителей);

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

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

19. 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).

20. 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

21. Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники в компьютерной сети Общества (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.

22. Допуск лиц к обработке персональных данных с использованием средств автоматизации осуществляется на при наличии паролей доступа.

23. 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.

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

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

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

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

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

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

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

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

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

26. Специфические требования по защите персональных данных в отдельных автоматизированных системах Общества 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

27. Все находящиеся на хранении и в обращении в Общества 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.

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

28.1. 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;

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

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

30. Общество осуществляет утилизацию съемных носителей персональных данных, твердых копий в порядке, определенном соответствующим локальным актом Общества.