

I. ПРЕАМБУЛА

При обработке персональных данных в рамках организации применяются принципы, предусмотренные международными актами — Всеобщей декларацией прав человека, Конвенцией о защите прав человека и основных свобод, Конвенцией о защите физических лиц при автоматизированной обработке персональных данных, Директивой 95/46/ЕС Европейского парламента и Совета о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также национальными нормативными актами — Конституцией Республики Молдова, Законом о защите персональных данных, Законом о доступе к информации, Требованиями к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства № 1123 от 14 декабря 2010 года, Положением о Реестре учета операторов персональных данных, утвержденным Постановлением Правительства № 296 от 15 мая 2012 года, и другими профильными законодательными и нормативными актами.

II. ВВЕДЕНИЕ

Компания «Business Market» SRL зарегистрирована по адресу: г. Яловены, ул. Григоре Виеру, № 18, Республика Молдова. При этом получение корреспонденции и местонахождение администрации осуществляется по адресу: мун. Кишинёв, ул. Александру чел Бун, № 108, Республика Молдова.

Настоящая Политика утверждена компанией «Business Market» SRL, которая осуществляет свою деятельность в соответствии с действующим законодательством Республики Молдова.

Настоящая Политика также утверждена в целях обеспечения соответствия деятельности компании «Business Market» SRL положениям Постановления Правительства Республики Молдова № 1123 от 14 декабря 2010 года «Об утверждении Требований к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Закона Республики Молдова № 133 от 08.07.2011 «О защите персональных данных».

III. ОБЩИЕ ПОНЯТИЯ

В настоящей Политике безопасности определены/используются следующие понятия:

персональные данные — любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (далее — субъект данных). Идентифицируемым физическим лицом является лицо, которое может быть идентифицировано прямо или косвенно, в частности посредством ссылки на такой идентификатор, как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор, либо на один или несколько элементов, характерных для его физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности;

обработка — любая операция или совокупность операций, осуществляемых с персональными данными или с наборами персональных данных, с использованием или без использования автоматизированных средств, таких как сбор, регистрация, организация, структурирование, хранение, адаптация или изменение, извлечение, консультация, использование, раскрытие посредством передачи, распространение или предоставление доступа иным способом, сопоставление или объединение, ограничение обработки, удаление или уничтожение;

ограничение обработки — маркировка хранящихся персональных данных с целью ограничения их дальнейшей обработки;

профилирование — любая форма автоматизированной обработки персональных данных, заключающаяся в использовании персональных данных для оценки определенных личных аспектов, относящихся к физическому лицу, в частности для анализа или прогнозирования

аспектов, связанных с производительностью на рабочем месте, экономическим положением, состоянием здоровья, личными предпочтениями, интересами, надежностью, поведением, местонахождением соответствующего физического лица или его перемещениями.

псевдонимизация — обработка персональных данных таким образом, чтобы они не могли быть отнесены к конкретному субъекту данных без использования дополнительной информации, при условии, что такая дополнительная информация хранится отдельно и в отношении нее применяются технические и организационные меры, обеспечивающие невозможность отнесения соответствующих персональных данных к идентифицированному или идентифицируемому физическому лицу;

система учета данных — любой структурированный набор персональных данных, доступных в соответствии с определенными критериями, независимо от того, является ли он централизованным, децентрализованным либо распределенным по функциональным или географическим критериям;

оператор — физическое или юридическое лицо, государственный орган, агентство или иной орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных. В случаях, когда цели и средства обработки определяются нормативными актами, оператор либо конкретные критерии его назначения устанавливаются соответствующими нормативными актами;

лицо, уполномоченное оператором — физическое или юридическое лицо, государственный орган, агентство или иной орган, осуществляющий обработку персональных данных от имени оператора;

местонахождение — место фактического и реального осуществления деятельности в рамках стабильных организационных условий;

получатель — физическое или юридическое лицо, государственный орган, агентство или иной орган, которому раскрываются персональные данные, независимо от того, является ли он третьей стороной или нет. Получателями не считаются государственные органы, которым персональные данные могут быть предоставлены в рамках определенного расследования в соответствии с нормативными актами; обработка этих данных соответствующими государственными органами осуществляется с соблюдением применимых норм в области защиты данных в соответствии с целями обработки;

третья сторона — физическое или юридическое лицо, государственный орган, агентство или орган, отличные от субъекта данных, оператора, лица, уполномоченного оператором, а также лиц, которые под непосредственным руководством оператора или лица, уполномоченного оператором, имеют право осуществлять обработку персональных данных;

согласие — любое свободно выраженное, конкретное, информированное и однозначное волеизъявление субъекта данных, посредством которого он путем заявления или иного недвусмысленного действия выражает согласие на обработку относящихся к нему персональных данных;

нарушение безопасности персональных данных — нарушение безопасности, которое случайно или незаконно приводит к уничтожению, утрате, изменению либо несанкционированному раскрытию передаваемых, хранящихся или иным образом обрабатываемых персональных данных либо к несанкционированному доступу к ним;

генетические данные — персональные данные, относящиеся к унаследованным или приобретенным генетическим характеристикам физического лица, которые предоставляют

уникальную информацию о физиологии или состоянии здоровья соответствующего лица и получены, в частности, в результате анализа образца биологического материала, взятого у данного лица;

биометрические данные — персональные данные, полученные в результате применения специальных методов обработки физических, физиологических или поведенческих характеристик физического лица, позволяющих или подтверждающих уникальную идентификацию данного лица, например изображения лица или дактилоскопические данные.

данные о состоянии здоровья — персональные данные, связанные с физическим или психическим здоровьем физического лица, включая предоставление медицинских услуг, которые раскрывают информацию о состоянии его здоровья;

национальный идентификационный номер — номер, посредством которого физическое лицо идентифицируется в определенных системах учета и который имеет общее применение, например: государственный идентификационный номер, серия и номер удостоверения личности, номер паспорта, номер водительского удостоверения;

представитель — физическое или юридическое лицо, имеющее местонахождение в Республике Молдова, назначенное в письменной форме оператором или лицом, уполномоченным оператором, на основании статьи 27, которое представляет оператора или лицо, уполномоченное оператором, в отношении обязательств, возложенных на них настоящим законом;

предприятие — физическое или юридическое лицо, осуществляющее экономическую деятельность, независимо от его организационно-правовой формы, включая партнерства или объединения, которые регулярно осуществляют экономическую деятельность;

группа предприятий — предприятие, осуществляющее контроль, и предприятия, находящиеся под его контролем;

обязательные корпоративные правила — политики в области защиты персональных данных, которые должны соблюдаться оператором или лицом, уполномоченным оператором, имеющим местонахождение на территории Республики Молдова, в отношении передачи или совокупности передач персональных данных оператору или лицу, уполномоченному оператором, в одном или нескольких государствах в рамках группы предприятий либо группы предприятий, участвующих в совместной экономической деятельности;

общий оборот — оборот в значении, определенном статьей 4 Закона о конкуренции № 183/2012;

услуги информационного общества — услуги в значении, определенном статьей 4 Закона № 284/2004 об услугах информационного общества;

прямой маркетинг — передача посредством телефона, почты или любых других средств прямой коммуникации рекламных или маркетинговых сообщений (для продвижения товаров или услуг), адресованных конкретным лицам;

международная организация — организация и ее подчиненные органы, регулируемые международным публичным правом, либо любой другой орган, учрежденный на основании соглашения, заключенного между двумя или более государствами, или в соответствии с таким соглашением.

персональные данные — любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъекту персональных данных). Идентифицируемым является лицо, которое может быть идентифицировано прямо или косвенно посредством ссылки на идентификационный номер либо на один или несколько элементов, характерных для его

физической, физиологической, психической, экономической, культурной или социальной идентичности;

специальные категории персональных данных — данные, раскрывающие расовое или этническое происхождение лица, его политические, религиозные или философские убеждения, социальную принадлежность, данные о состоянии здоровья или половой жизни, а также данные, относящиеся к уголовным осуждениям, процессуальным мерам принуждения или административным санкциям.

оператор — физическое лицо или юридическое лицо публичного либо частного права, включая государственный орган, любое другое учреждение или организацию, которые самостоятельно или совместно с другими определяют цели и средства обработки персональных данных, прямо предусмотренные действующим законодательством;

лицо, уполномоченное оператором — физическое лицо или юридическое лицо публичного либо частного права, включая государственный орган и его территориальные подразделения, которое осуществляет обработку персональных данных от имени и по поручению оператора на основании полученных от оператора инструкций;

аутентификация — проверка идентификатора, присвоенного субъекту доступа, и подтверждение его подлинности;

контроль безопасности — действия, предпринимаемые компанией «Business Market» SRL в целях обеспечения надлежащего уровня безопасности персональных данных, обрабатываемых в информационных системах и/или ведущихся реестрах;

временные файлы — совокупность данных или информации на цифровом носителе, создаваемая на ограниченный период времени до начала выполнения задач, для которых они были предназначены;

идентификация — присвоение идентификатора субъектам и объектам доступа и/или сопоставление представленного идентификатора со списком присвоенных идентификаторов;

целостность — достоверность, непротиворечивость и актуальность информации, содержащей персональные данные, а также ее защита от уничтожения и несанкционированного изменения;

средства криптографической защиты информации, содержащей персональные данные — технические, программные и программно-технические средства, системы и комплексы систем, реализующие алгоритмы криптографического преобразования информации, содержащей персональные данные, предназначенные для обеспечения целостности и конфиденциальности информации в процессе ее обработки, хранения и передачи по каналам связи;

уровень защиты — уровень безопасности, соразмерный риску, связанному с обработкой соответствующих персональных данных, а также с рисками для прав и свобод физических лиц, разработанный и обновляемый с учетом уровня технологического развития и затрат на внедрение соответствующих мер;

политика безопасности персональных данных — документ, разработанный оператором персональных данных — «Business Market» SRL, содержащий точное описание мер безопасности и выбранных средств защиты данных, с учетом потенциальных угроз для обрабатываемых персональных данных и реальных рисков, которым они подвергаются;

периметр безопасности — зона, представляющая собой барьер для прохода, оборудованный средствами физического и/или технического контроля доступа.

ответственное лицо за политику безопасности персональных данных — лицо, ответственное за надлежащее функционирование комплексной системы защиты информации, содержащей персональные данные, а также за разработку, внедрение и контроль соблюдения положений политики безопасности владельца персональных данных;

защита информации от непреднамеренных воздействий — совокупность мер, направленных на предотвращение непреднамеренных действий, вызванных ошибками пользователя, неисправностями технических и программно-технических средств, природными явлениями или иными причинами, которые непосредственно не направлены на изменение информации, но приводят к ее искажению, уничтожению, копированию, блокированию доступа к информации, а также к ее утрате, уничтожению либо повреждению материального носителя информации, содержащей персональные данные;

носитель персональных данных — магнитный, оптический, лазерный, бумажный или иной носитель информации, на котором создается, фиксируется, передается, принимается, хранится либо иным образом используется документ и который позволяет воспроизводить его содержание;

восстановление данных — процедуры по воссозданию/восстановлению персональных данных до состояния, в котором они находились до момента их утраты или уничтожения;

информационная технология — совокупность методов, способов и средств обработки и передачи информации, содержащей персональные данные, а также правил их применения;

пользователь — лицо, действующее под руководством владельца персональных данных и имеющее признанное право доступа к информационным системам персональных данных;

рабочая сессия — период времени с момента запуска компьютера и приложения для использования информационного ресурса либо с момента запуска информационного ресурса до момента их остановки;

информационная система персональных данных — совокупность взаимосвязанных информационных ресурсов и технологий, методов и персонала, предназначенных для хранения, обработки и предоставления информации, содержащей персональные данные;

обработка персональных данных — любая операция или совокупность операций, осуществляемых с персональными данными посредством автоматизированных или неавтоматизированных средств, таких как сбор, регистрация, организация, хранение, сохранение, восстановление, адаптация или изменение, извлечение, ознакомление, использование, раскрытие посредством передачи, распространение или предоставление иным способом, присоединение или объединение, блокирование, удаление или уничтожение;

хранение — сохранение персональных данных на любом виде носителя;

система учета персональных данных — любая структурированная совокупность персональных данных, доступных в соответствии с определенными критериями, независимо от того, является ли она централизованной, децентрализованной либо распределенной по функциональным или географическим критериям;

согласие субъекта персональных данных — любое свободное, выраженное и безусловное волеизъявление в письменной или электронной форме, соответствующей требованиям к электронному документу, посредством которого субъект персональных данных дает согласие на обработку относящихся к нему данных;

обезличивание данных — изменение персональных данных таким образом, чтобы сведения о личных или материальных обстоятельствах более не позволяли отнести их к идентифицированному или идентифицируемому физическому лицу либо позволяли осуществить такое отнесение только в рамках расследования, требующего несоразмерных затрат времени, средств и трудовых ресурсов.

IV. Цели Политики безопасности

Основными целями настоящей Политики являются доступность, целостность и конфиденциальность всей информации, включая персональные данные, обрабатываемые компанией «Business Market» SRL, как в процессе ручной обработки, так и в рамках информационных систем и технологических процессов.

Безопасность является важнейшей составляющей оптимального функционирования процессов, основанных на информационных технологиях, в компании «Business Market» SRL. Основой надлежащего уровня IT-безопасности является соблюдение настоящей Политики.

Настоящая Политика устанавливает требования и правила защиты всей информации, включая персональные данные, информационных систем и IT-процессов от природных воздействий, человеческих и технических ошибок, а также от преднамеренных действий, которые могут причинить материальный или нематериальный ущерб либо привести к нарушениям законодательства.

Учитывая, что безопасность информационных технологий не может быть гарантирована исключительно с помощью технических систем, настоящая Политика также охватывает организационно-правовые и иные аспекты обеспечения безопасности.

Компания «Business Market» SRL обеспечивает защиту персональных данных как участников процесса/посетителей, так и своих работников.

Положения настоящей Политики являются минимальным стандартом безопасности для компании «Business Market» SRL, в том числе для всех работников компании.

Исходя из настоящих положений, все работники компании «Business Market» SRL обязаны строго соблюдать требования настоящей Политики и внутренние правила компании, касающиеся защиты персональных данных и IT-систем.

V. Положения об иерархии и ответственности лица, ответственного за Политику безопасности

Оператор персональных данных, исходя из специфики своей деятельности, посредством настоящей Политики безопасности устанавливает необходимые процедуры и меры для обеспечения надлежащего уровня защиты при обработке персональных данных в рамках управляемых систем учета.

Политика безопасности персональных данных подлежит пересмотру не реже одного раза в год в результате изменений или переоценки полномочий организации. На руководителей возлагается обязанность назначить лицо (лиц), которое непосредственно осуществляет корректировку положений настоящего документа.

Политика безопасности в обязательном порядке доводится под подпись до сведения всех работников, ответственных за обработку персональных данных, до предоставления им доступа к обработке персональных данных, а также при внесении изменений, обусловленных необходимостью обеспечения надлежащего уровня защиты персональных данных.

Ответственным за внедрение и контроль соблюдения положений Политики безопасности персональных данных назначается лицо, которое в соответствии с должностной инструкцией

и/или внутренним приказом располагает достаточными ресурсами (временем, кадровыми ресурсами, оборудованием и бюджетом) и имеет свободный доступ к необходимой для выполнения своих функций информации в той мере, в которой такой доступ не выходит за рамки настоящей Политики.

Назначенное ответственное лицо, независимо от выполняемых функций, в рамках контроля за внедрением/соблюдением положений Политики безопасности непосредственно подчиняется руководителю компании «Business Market» SRL либо лицу, исполняющему обязанности руководителя.

Лицо, ответственное за Политику безопасности персональных данных, обеспечивает четкое распределение различных обязанностей в области безопасности обработки персональных данных (предотвращение, надзор, выявление и реагирование), а также их выполнение независимо от давления, обусловленного личными интересами или иными обстоятельствами.

Лицо, ответственное за Политику безопасности персональных данных, четко определяет обязанности и процессы управления безопасностью персональных данных, обеспечивая их надлежащую интеграцию в общую организационную и функциональную структуру; обеспечивает необходимые технические и организационные меры для организации процесса управления безопасностью персональных данных; разрабатывает процедуры классификации информации, содержащей персональные данные, таким образом, чтобы можно было составить номенклатуру и определить местонахождение всех обрабатываемых персональных данных независимо от типа носителя данных; проводит обучение лиц, участвующих в процессе обработки персональных данных, с целью надлежащего выполнения ими своих функциональных обязанностей и принятия на себя ответственности за безопасность персональных данных, включая обеспечение их конфиденциальности.

VI. Средства, на которые распространяются принципы защиты персональных данных

Защита персональных данных в компании «Business Market» SRL (в качестве оператора персональных данных) обеспечивается посредством комплекса технических и организационных мер, направленных на предотвращение незаконной обработки персональных данных.

Специальными средствами и методами защиты охватываются все управляемые информационные ресурсы оператора персональных данных, содержащие персональные данные, хранящиеся на:

магнитных, оптических, лазерных и иных электронных носителях информации, в информационных массивах и базах данных;

информационных системах, сетях, операционных системах, системах управления базами данных и других приложениях, телекоммуникационных системах, включая средства создания и тиражирования документов, а также другие технические средства обработки информации.

VII. Меры по защите персональных данных обеспечиваются в целях:

предотвращения утечки информации, содержащей персональные данные, посредством исключения несанкционированного доступа к ней;

предотвращения несанкционированного уничтожения, изменения, копирования или блокирования персональных данных в телекоммуникационных сетях и информационных ресурсах;

недопущения раскрытия третьим лицам информации с ограниченным доступом;

повышения эффективности использования информационных ресурсов как на бумажных носителях, так и в электронном формате.

VIII. Защита персональных данных, обрабатываемых в информационных системах, осуществляется следующими методами:

предотвращение несанкционированных подключений к телекоммуникационным сетям и перехвата с помощью технических средств персональных данных, передаваемых по этим сетям;

исключение несанкционированного доступа к обрабатываемым персональным данным;

предотвращение специальных технических и программных воздействий, которые могут привести к уничтожению или изменению персональных данных либо к сбоям в работе технического и программного комплекса;

предотвращение преднамеренных и/или непреднамеренных действий внутренних и/или внешних пользователей, а также других работников оператора/лиц, уполномоченных оператором, которые могут привести к уничтожению или изменению персональных данных либо к сбоям в работе технического и программного комплекса;

предотвращение утечки информации, содержащей персональные данные, передаваемой по каналам связи, обеспечивается посредством применения методов шифрования данной информации, а также использования VPN-каналов;

предотвращение уничтожения, изменения персональных данных или сбоев в работе программного обеспечения, предназначенного для обработки персональных данных, обеспечивается посредством использования специальных технических и программных средств защиты, включая лицензионное программное обеспечение, антивирусные программы, организацию системы контроля безопасности программного обеспечения и регулярное резервное копирование данных;

предотвращение утечки информации, содержащей персональные данные, обеспечивается посредством постоянного внутреннего аудита информационных систем;

четкое установление порядка доступа к информации, содержащей персональные данные, обрабатываемой в информационных и учетных системах, как для внутренних, так и для внешних пользователей.

IX. Организационные и технические процедуры, подлежащие соблюдению в компании «Business Market» SRL при обработке персональных данных

1. Общие меры по управлению информационной безопасностью

a) В случае временного неиспользования бумажных или электронных (цифровых) носителей информации, содержащих персональные данные, они хранятся в сейфах или запираемых металлических шкафах.

b) Компьютеры, терминалы доступа и принтеры отключаются по завершении рабочих сессий.

c) Обеспечивается безопасность пунктов приема/отправки корреспонденции, а также защита факсимильных и копировальных аппаратов от несанкционированного доступа.

d) Обеспечивается безопасность и физический доступ к средствам отображения информации, содержащей персональные данные, с целью предотвращения ее просмотра неуполномоченными лицами.

e) Средства обработки персональных данных, информация, содержащая персональные данные, или программное обеспечение, предназначенное для обработки персональных данных, выносятся за пределы периметра безопасности только на основании письменного разрешения руководства.

f) Все программы, используемые в информационной системе, должны соответствовать условиям лицензирования.

g) Установка программ типа Shareware или freeware без разрешения администратора информационной системы запрещается.

2. Безопасность физической среды и информационных технологий, используемых в процессе обработки персональных данных

a) Доступ в здания/офисы/кабинеты или помещения, где размещены информационные системы персональных данных, ограничивается и предоставляется только лицам, имеющим соответствующее разрешение, согласно установленному списку или соответствующим идентификационным средствам (значкам, пропускам, идентификационным картам).

b) Обеспечивается управление и мониторинг физического доступа во всех точках доступа к информационным системам персональных данных, включая реагирование на нарушения установленного режима доступа.

c) Периметр безопасности компании «Business Market» SRL представляет собой территорию офисных помещений, в которых осуществляется обработка/хранение персональных данных.

d) Периметр здания или помещений, в которых размещены средства обработки персональных данных, является физически целостным; наружные стены помещений являются прочными, а входы оборудованы замками и системой сигнализации.

e) Размещение средств обработки персональных данных осуществляется с учетом необходимости обеспечения их защиты от несанкционированного доступа, краж, пожаров, затоплений и других возможных рисков.

f) Двери и окна запираются в случае отсутствия сотрудников в помещении.

g) Компьютеры, серверы и другие терминалы доступа размещаются в местах с ограниченным доступом для посторонних лиц.

h) Доступ в периметр безопасности здания компании «Business Market» SRL, где осуществляется обработка/хранение персональных данных, с несанкционированным фото-/видеооборудованием запрещается, с учетом необходимости обеспечения режима конфиденциальности и безопасности обработки персональных данных, предусмотренного статьями 29 и 30 Закона о защите персональных данных, а также пунктом 26 Требований.

i) Использование фото-, видео-, аудио- и других средств записи в пределах периметра безопасности допускается только при наличии специального разрешения руководства.

3. Идентификация и аутентификация пользователей

a) Осуществляются идентификация и аутентификация пользователей информационных систем персональных данных, а также процессов, выполняемых от имени этих пользователей.

b) Все пользователи (включая персонал, обеспечивающий техническую поддержку, сетевых администраторов, программистов и администраторов баз данных) имеют персональный идентификатор (ID пользователя), который не содержит признаков, указывающих на уровень доступа пользователя.

с) Для подтверждения ID пользователя используются пароли, специальные физические средства доступа с памятью (токены) или микропроцессорные карты, а также биометрические средства аутентификации, основанные на уникальных и индивидуальных характеристиках лица.

д) В случае прекращения, приостановления или изменения трудового договора/служебных отношений пользователя, если новые обязанности не требуют доступа к персональным данным, либо в случае изменения прав доступа пользователя, злоупотребления предоставленными кодами в целях совершения противоправного деяния или длительного отсутствия пользователя, идентификационные и аутентификационные коды отзываются или приостанавливаются IT-администратором.

4. Идентификация и аутентификация оборудования

Обеспечивается возможность идентификации и аутентификации оборудования, используемого при операциях по обработке персональных данных, с сохранением соответствующей информации в течение длительного периода времени.

5. Управление идентификаторами пользователей

Управление идентификаторами пользователей включает:

однозначную идентификацию каждого пользователя;

проверку подлинности каждого пользователя.

6. Использование паролей в процессе обеспечения информационной безопасности

При выборе и использовании паролей соблюдаются правила обеспечения информационной безопасности, включающие:

сохранение конфиденциальности паролей;

запрет записи паролей на бумажном носителе в случае, если не обеспечена безопасность его хранения;

изменение паролей каждый раз при наличии признаков возможной компрометации системы или пароля;

выбор надежных паролей длиной не менее 8 символов, которые не связаны с персональной информацией пользователя, не содержат одинаковых последовательных символов и не состоят полностью из групп цифр или букв;

изменение паролей каждые 3 месяца;

отключение функции автоматической регистрации/входа с использованием сохраненных паролей.

7. Контроль управления доступом

Осуществляется систематический контроль действий пользователей с целью оценки правильности и соответствия установленным требованиям операций и действий, выполняемых посредством информационных систем персональных данных.

8. Удаленный доступ

а) Все методы удаленного доступа к информационным системам персональных данных защищаются (с использованием VPN, шифрования, криптографических средств и т. д.), а также документируются, подвергаются мониторингу и контролю

б) Каждый метод удаленного доступа к информационным системам персональных данных санкционируется ответственными лицами компании «Business Market» SRL и предоставляется только тем пользователям, которым такой доступ необходим для выполнения установленных задач.

9. Ограничение использования беспроводных технологий

а) Беспроводной доступ к информационным системам персональных данных максимально ограничивается, документируется и подвергается мониторингу и контролю

б) Беспроводной доступ к информационным системам персональных данных разрешается только при использовании криптографических средств защиты информации.

с) Использование беспроводных технологий санкционируется ответственными лицами компании «Business Market» SRL.

10. Электроэнергетическая безопасность

а) Электрическое оборудование, используемое для обеспечения функционирования информационных систем персональных данных, а также электрические кабели защищаются от повреждений и несанкционированного подключения путем их размещения в специальных нишах.

б) В случае возникновения чрезвычайных, аварийных ситуаций или обстоятельств непреодолимой силы обеспечивается возможность отключения электропитания информационных систем персональных данных, включая возможность отключения любого IT-компонента.

с) В офисах, где размещены информационные системы персональных данных и средства обработки персональных данных, внедрены автоматизированные системы обнаружения и сигнализации о пожаре.

11. Контроль установки и вывода из эксплуатации IT-компонентов

а) Осуществляется контроль и ведется учет установки и вывода из эксплуатации программных, технических и программно-технических средств, используемых в информационных системах персональных данных.

б) Информация, содержащая персональные данные и хранящаяся на носителях информации, подлежит физическому уничтожению либо безопасной перезаписи и уничтожению с использованием надежных методов, исключающих использование стандартных функций удаления.

12. Раскрытие персональных данных

а) При раскрытии электронного формата персональных данных, содержащихся в системах учета, посредством коммуникационных сетей либо на других цифровых носителях хранения и сохранения должна обеспечиваться шифровка этой информации либо рассматриваться возможность использования двустороннего соединения посредством защищенного VPN-канала.

Беспроводной доступ к системам учета персональных данных разрешается только авторизованным пользователям.

Каждый случай запроса на раскрытие персональных данных посредством их электронной передачи рассматривается отдельно, исходя из технических возможностей, обеспечиваемых

получателем и оператором, а также в соответствии с организационными и техническими мерами, внедренными сторонами.

В случае если коммуникационные сети представляют угрозу конфиденциальности и безопасности персональных данных, используются традиционные способы передачи (почтовое отправление с уведомлением о вручении, личная передача и т. д.).

b) Раскрытие персональных данных посредством передачи через коммуникационные сети, которые не соответствуют установленным Требованиям (например, отправка информации через личные электронные почтовые ящики типа @gmail.com, @mail.ru, @yahoo.com и т. д.), запрещается.

c) Запрещаются операции по раскрытию персональных данных между компанией «Business Market» SRL и другими организациями, географически расположенными на левом берегу Днестра, которые отказываются юридически подчиняться законодательству Республики Молдова, исходя из того, что в настоящее время отсутствует возможность осуществления эффективного контроля над данной территорией, в том числе в части соблюдения требований законодательства о защите персональных данных.

d) Процедура раскрытия посредством передачи персональных данных, хранящихся на бумажных и/или цифровых носителях, за пределы Республики Молдова должна регулироваться внутренним нормативным актом и/или двусторонним соглашением с учетом необходимости обеспечения надлежащего уровня защиты персональных данных.

e) Трансграничная передача персональных данных осуществляется в строгом соответствии с положениями статьи 32 Закона о защите персональных данных, в частности в случаях, когда международный договор, на основании которого осуществляется передача, не содержит гарантий защиты прав субъекта персональных данных.

f) Объем и категории персональных данных, собираемых в целях ведения учета в компании «Business Market» SRL, ограничиваются строго необходимым минимумом для достижения заявленных целей.

g) Доступ к информационным системам, находящимся в ведении компании «Business Market» SRL, со стороны Генеральной прокуратуры (в соответствующих случаях — территориальных/специализированных прокуратур), Министерства внутренних дел, Национального центра по борьбе с коррупцией и т. д. допускается только в случае, если соответствующий запрос отвечает требованиям статей 15 и 212 Уголовно-процессуального кодекса.

Разъясняется, что в соответствии с положениями статьи 157 Уголовно-процессуального кодекса, документы в любой форме (письменной, аудио-, видео-, электронной и т. д.), исходящие от физических или юридических лиц, если в них изложены либо подтверждены обстоятельства, имеющие значение для дела, в том числе информация, содержащаяся в аудите информационных и учетных систем, могут быть затребованы посредством запроса органа уголовного преследования в рамках уголовного расследования либо в процессе рассмотрения дела судом.

В данном случае, однако, должны соблюдаться положения статьи 214 Уголовно-процессуального кодекса, согласно которым в ходе уголовного процесса не допускается без необходимости сбор, использование и распространение официальной информации с ограниченным доступом.

Лица, которым орган уголовного преследования или суд предлагает сообщить либо предоставить официальную информацию с ограниченным доступом (в том числе операторы персональных данных), имеют право убедиться в том, что соответствующие данные собираются именно для

целей данного уголовного производства, а в противном случае — отказаться от их сообщения или предоставления.

Лица, которым орган уголовного преследования или суд предлагает сообщить либо предоставить официальную информацию с ограниченным доступом, имеют право предварительно получить от лица, запрашивающего информацию, письменное разъяснение, подтверждающее необходимость предоставления указанных данных.

Следует учитывать, что в соответствии с положениями статьи 8 Закона о доступе к информации, персональные данные относятся к категории официальной информации с ограниченным доступом, доступ к которой осуществляется в соответствии с законодательством о защите персональных данных.

В случае если адвокат или уполномоченное лицо запрашивает возможность ознакомиться с личным делом клиента, им в письменной форме разъясняются обязанности, предусмотренные статьей 15 Уголовно-процессуального кодекса, статьями 29 и 30 Закона о защите персональных данных, а также ответственность, предусмотренная статьей 74¹ Кодекса о правонарушениях.

13. Права субъектов персональных данных

а) В случае если персональные данные собираются непосредственно у субъекта данных, в соответствии с положениями статьи 12 Закона о защите персональных данных, лицу должна быть предоставлена следующая информация, за исключением случаев, когда оно уже располагает соответствующей информацией:

об идентичности оператора или, в соответствующих случаях, лица, уполномоченного оператором (наименование, юридический адрес, IDNO, регистрационный номер в Реестре учета операторов персональных данных);

о конкретной цели обработки собираемых персональных данных;

о получателях или категориях получателей персональных данных;

о наличии права на получение информации и доступа к собранным данным;

о праве на внесение изменений в данные, в частности на исправление, обновление, блокирование или удаление персональных данных, обработка которых противоречит закону вследствие их неполноты или неточности;

о праве на возражение (оппозицию), а также об условиях осуществления указанных прав;

о том, являются ли ответы на вопросы, посредством которых собираются данные, обязательными или добровольными, включая возможные последствия отказа отвечать на вопросы, посредством которых собирается информация.

б) Субъектам персональных данных обеспечивается право доступа и возможность ознакомиться с документами, составленными в отношении них, с целью проверки правильности их оформления, обжалования невключения или неправильного включения отдельных данных, а также других ошибок, допущенных при внесении сведений о них.

При этом лица, ответственные за обработку персональных данных, обеспечивают доступ лица только к тем персональным данным, которые непосредственно относятся к нему.

Возможность ознакомления с персональными данными других субъектов, содержащимися в личных делах или иных материалах, исключается, за исключением случаев, когда заявители

реализуют законный интерес, который не наносит ущерба интересам, правам и основным свободам субъекта персональных данных.

с) Право на получение информации обеспечивается оператором персональных данных (либо организациями, обеспечивающими техническое обслуживание системы и/или предоставляющими оператору услуги на условиях аутсорсинга) всем лицам, чьи данные подвергаются обработке.

d) В случае реализации субъектом персональных данных права на внесение изменений неточные данные обновляются путем исправления или удаления. Основанием для таких изменений могут служить только законные источники (удостоверения личности, акты гражданского состояния, основные государственные информационные ресурсы и т. д.). Соответствующие изменения должны быть внесены во все управляемые информационные и учетные системы.

14. Хранение, сохранение и уничтожение обрабатываемых персональных данных

a) Доступ в помещения/периметр, где размещены информационные и учетные системы персональных данных, ограничивается и разрешается только лицам, имеющим соответствующее разрешение в соответствии с институциональной политикой безопасности/утвержденными ведомственными регламентами.

b) Запрещается хранение и сохранение электронного формата персональных данных, структурированных в учетных системах, на компьютерах, подключенных к Интернету, если они не оснащены специальными техническими и программными средствами защиты и на них не установлены лицензионное программное обеспечение, антивирусные программы, системы контроля безопасности программного обеспечения, средства регулярного резервного копирования и проведения аудита.

с) Запрещается вносить на территорию институционального периметра безопасности и использовать в служебных целях личные компьютеры или собственные носители информации.

Кроме того, доступ к служебным компьютерам защищается/ограничивается путем создания пользовательских профилей, а права администратора предоставляются только лицу, ответственному за реализацию политики безопасности, назначенному в компании «Business Market» SRL

d) Хранение персональных данных на магнитных, оптических, лазерных, бумажных и иных носителях информации обеспечивается путем их размещения в сейфах или запирающихся металлических шкафах.

Несанкционированный вынос носителей персональных данных за пределы периметра безопасности оператора запрещается.

15. Аудит управляемых информационных систем

a) Осуществляется регистрация попыток входа/выхода пользователя из системы со следующими параметрами:

дата и время попытки входа/выхода;

ID пользователя;

результат попытки входа/выхода — положительный или отрицательный.

b) Осуществляется регистрация попыток получения доступа (выполнения операций) к приложениям и процессам, предназначенным для обработки персональных данных, со следующими параметрами:

дата и время попытки получения доступа/выполнения операции;

наименование (идентификатор) приложения или процесса;

ID пользователя;

характеристики защищаемого ресурса (идентификатор, логическое имя, имя файла, номер и т. д.);

тип запрошенной операции (чтение, запись, удаление и т. д.);

результат попытки получения доступа/выполнения операции — положительный или отрицательный.

с) Осуществляется регистрация изменений прав доступа (полномочий) пользователя и статуса объектов доступа со следующими параметрами:

дата и время изменения полномочий;

ID администратора, осуществившего изменения;

ID пользователя и его полномочия либо описание объектов доступа и их новый статус.

d) Осуществляется регистрация вывода из системы информации, содержащей персональные данные (электронных документов, данных и т. д.), а также изменений прав доступа субъектов и статуса объектов доступа со следующими параметрами:

дата и время выдачи;

наименование информации и пути доступа к ней;

указание оборудования (устройства), предоставившего информацию (логическое имя);

ID пользователя, запросившего информацию.

16. Обеспечение защиты от вредоносных программ (вирусов)

Обеспечивается защита от проникновения вредоносных программ в программное обеспечение, предназначенное для обработки персональных данных, путем использования лицензионных антивирусных программ.

17. Тестирование функциональных возможностей обеспечения безопасности информационных систем персональных данных

Обеспечивается тестирование корректного функционирования функций безопасности информационных систем персональных данных:

автоматически при запуске системы;

ежемесячно — по запросу уполномоченного пользователя.

18. Управление инцидентами безопасности

а) Персонал, обеспечивающий эксплуатацию информационных систем персональных данных, проходит не реже одного раза в год обучение по вопросам ответственности и обязанностей при выполнении мероприятий по управлению инцидентами безопасности и реагированию на них.

b) Персонал компании «Business Market» SRL обязан незамедлительно информировать руководство об инцидентах, нарушающих безопасность информационных систем персональных данных.

c) Обработка инцидентов включает:

выявление;

анализ;

предотвращение дальнейшего развития;

устранение;

восстановление безопасности.

d) До 31 января каждого года оператор персональных данных письменно информирует Национальный центр по защите персональных данных о выявленных инцидентах безопасности.

e) В случае возникновения инцидентов безопасности в компании «Business Market» SRL ответственное лицо принимает необходимые меры для установления источника возникновения инцидента, проводит его анализ и устраняет причины инцидента безопасности.

О возникшем инциденте Национальный центр по защите персональных данных Республики Молдова информируется в течение 72 часов с момента возникновения инцидента.

f) В рамках проверок, проводимых Национальным центром по защите персональных данных Республики Молдова, ему предоставляется необходимая поддержка и обеспечивается доступ к информации, необходимой и относящейся к предмету проверки.

19. Маркировка документов

Вся информация, которая предполагается к раскрытию и содержит персональные данные, должна быть маркирована с указанием регистрационного номера из Реестра учета операторов персональных данных.

Пример:

Внимание! Документ содержит персональные данные, обрабатываемые в рамках системы учета № 000000X-00X, зарегистрированной в Реестре учета операторов персональных данных www.registru.datepersonale.md. Дальнейшая обработка этих данных может осуществляться только на условиях, предусмотренных Законом № 133 от 08.07.2011 о защите персональных данных.

20. Ответственность за обеспечение безопасности персональных данных и информации ограниченным доступом

Оператор персональных данных, лицо, уполномоченное оператором, а в соответствующих случаях — третьи лица, подписавшие Приложение № 1, за несоблюдение положений настоящей Политики безопасности несут гражданскую, административную и уголовную ответственность в соответствии с законодательством Республики Молдова:

гражданскую — в соответствии с Гражданским кодексом;

административную/контравенционную — в соответствии со статьей 741 Кодекса о правонарушениях;

уголовную — в соответствии со статьями 177, 178 и 180 Уголовного кодекса.