ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

СОДЕРЖАНИЕ:

В соответствии с положениями ЗАКОНА № 133 от 08.07.2011 г. «О защите персональных данных», SC ”Totul pentru copii” SRLобрабатывает персональные данные с соблюдением указанных далее принципов, в законных целях.

Обработка персональных данных осуществляется смешанными средствами (ручными и автоматическими), с соблюдением законных требований и в условиях, обеспечивающих безопасность, конфиденциальность и соблюдение прав соответствующего лица.

1. СБОР ПЕРСОНАЛЬНЫХ ДАННЫХ

Цель данной политики безопасности состоит в обеспечении надлежащего уровня защиты персональных данных соответствующих лиц, путем надлежащего применения национального законодательства о защите данных и конфиденциальности сообщения.

2. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Нотификация:

Оператор персональных данных нотифицирован в Национальном центре по защите персональных данных РМ;

Законность:

Обработка персональных данных осуществляется добросовестно и на основании, и в соответствии с законными положениями;

Четко определенная цель:

Любая обработка персональных данных осуществляется в четко определенных, ясных и законных, адекватных целях, приемлемых и нечрезмерных по отношению к цели, с которой они собираются и в дальнейшем обрабатываются;

Осведомление:

Настоящим осведомлением лица знакомятся с тем, что будут обрабатываться их персональные данные;

Хранение:

Персональные данные не хранятся дольше времени, необходимого для выполнения целей, в которых они были собраны;

Защита соответствующих лиц:

Обработка персональных данных осуществляется уполномоченными лицами компанииSC ”Totul pentru copii” SRL, или иными лицами, уполномоченными на законных основаниях.

Безопасность:

Технические и организационные меры безопасности персональных данных устанавливаются для защиты персональных данных от случайного или незаконного уничтожения, утери, изменения, разглашения или несанкционированного доступа (доступ к базам данных осуществляется на основе имени пользователя и пароля, и регулируется ролями и правами доступа). Возможность порчи открываемых данных предотвращается посредством firewall, отслеживаемого SC ”Totul pentru copii” SRL, а также постоянно обновляемыми антивирусными решениями. Передача между серверами клиентов и администраторам, и операторам производится криптированно, на основе цифрового сертификата, таким образом, данные не могут быть перехвачены.

3. ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с положениями ЗАКОНА № 133 от 08.07.2011 г. «О защите персональных данных», SC ”Totul pentru copii” SRLобязано управлять в условиях безопасности и только в изложенных ниже целях, предоставляемыми ему персональными данными.

SC ”Totul pentru copii” SRL обязуется соблюдать конфиденциальность персональных данных, предоставленных через сайт www.baby-boom.md, как это предусматривают положения ЗАКОНА № 133 от 08.07.2011 г., с последующими изменениями, о защите персональных данных.

4. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Представляют особые риски для прав и свобод лиц следующие операции по обработке персональных данных:

1) адаптация, изменение, раскрытие посредством передачи, распространения или любым иным способом персональных данных, связанных с расовой или национальной принадлежностью, политическими, религиозными убеждениями, принадлежностью к политической партии или религиозной организации, персональных данных о состоянии здоровья или интимной жизни, а также персональных данных, касающихся уголовных наказаний, мер пресечения, дисциплинарных или административных взысканий;

2) операции по обработке генетических, биометрических данных и данных, которые позволяют определить географическое местонахождение лиц через сети электронной связи;

3) операции по обработке персональных данных с помощью электронных средств, предназначенной для оценки некоторых личных аспектов, таких как профессиональная компетенция, надежность, поведение и т.п.;

4) операции по обработке персональных данных с помощью электронных средств в системах учета, для анализа кредитоспособности, финансово-экономического положения, деяний, которые

могут повлечь дисциплинарную, правонарушительную или уголовную ответственность физических лиц;

5) операции по обработке персональных данных несовершеннолетних для коммерческих целей (прямого маркетинга);

6) операции по обработке персональных данных, указанных в пунктах 1) и 2) настоящего приложения, а также персональных данных несовершеннолетних, собираемых посредством Интернета или электронной почты.

Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (в дальнейшем - Требования) направлены на установление минимальных правил внедрения держателями персональных данных необходимых технических и организационных мер по обеспечению безопасности, конфиденциальности и целостности персональных данных, обрабатываемых в рамках информационных систем персональных данных и/или реестрах, которые ведутся вручную, в соответствии с положениями Закона №17-XVI от 15 февраля 2007 г. «О защите персональных данных» (Официальный монитор Республики Молдова, 2007 г., №107-111, ст.468) и Закона № 71-XVI от 22 марта 2007 г. «О регистрах» (Официальный монитор Республики Молдова, 2007 г., №70-73, ст.314).

Настоящие Требования создают необходимую основу для применения Конвенции о защите лиц при автоматизированной обработке персональных данных, заключенной в Страсбурге 28 января 1981 г., опубликованной в European Treaty Series, № 108, ратифицированной Республикой Молдова Постановлением Парламента № 483-XIV от 2 июля 1999 г.

Согласно Постановлению № 1123 от 14.12.2010 г. «Об утверждении Требований по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», меры по защите персональных данных являются составной частью работ по созданию, развитию и эксплуатации информационной системы персональных данных и непрерывно выполняются всеми держателями персональных данных. Защита персональных данных в информационных системах персональных данных обеспечивается комплексом организационных и технических мер по предупреждению неправомерной обработки персональных данных. Меры по защите персональных данных, обрабатываемых в информационных системах персональных данных, применяются исходя из необходимости обеспечения конфиденциальности этих мер. Осуществление любых мер и работ с использованием информационных ресурсов держателя персональных данных запрещено в случаях, если не приняты и не выполнены соответствующие меры по защите персональных данных.

SC ”Totul pentru copii” SRL подтверждает, что выполняет минимальные требования к безопасности персональных данных.

SC ”Totul pentru copii” SRL использует методы и технологии безопасности, вместе с политиками, применяемые к участникам, и рабочие процедуры, в том числе, контроля и аудита, для защиты собираемых персональных данных согласно действующим законным положениям. Передача между сервером клиентов и администраторам, и операторам производится через криптированно, на основе цифрового сертификата, таким образом, данные не могут быть перехвачены. Персональные данные по заказам хранятся закодировано в базе данных оператора.

Согласно Постановлению № 1123 от 14.12.2010 г., защита персональных данных в информационных системах персональных данных обеспечивается с целью:

1) предотвращения утечки информации, содержащей персональные данные путем исключения несанкционированногодоступа к ней;

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

3) соблюдения нормативно - правовой базы по использованию информационных систем и программ для обработки персональных данных;

4) обеспечения исчерпывающего, целостного и достоверного характера персональных данных в телекоммуникационных сетях и информационных ресурсах;

5) сохранения возможностей по управлению процессом обработки и хранения персональных данных.

Защита персональных данных, обрабатываемых в информационных системах, проводится методами:

1) предотвращения неавторизированного подключения к телекоммуникационным сетям и перехвата с помощью технических средств персональных данных, передаваемых по этим сетям;

2) исключения несанкционированного доступа к обработанным персональным данным;

3) предотвращения специальных технических и программных действий, которые обуславливают уничтожение, изменение персональных данных или сбой в работе технического и программного комплекса;

4) предотвращения преднамеренных и/или непреднамеренных действий внутренних и/или внешних пользователей, а также других сотрудников держателя персональных данных, которые обуславливают уничтожение, изменение персональных данных или сбой в работе технического и программного комплекса.

Доступ в помещения/офисы/кабинеты или места, где расположены информационные системы персональных данных, ограничен и разрешен только лицам, имеющим необходимое разрешение, и только в рабочее время, согласно списку и соответствующим отличительным знакам (эмблемы, значки, идентификационные карты, микропроцессорные карты). Помещения, в которых установлены информационные системы персональных данных, оснащаются системами контроля доступа и видеонаблюдения с целью отслеживания доступа лиц в эти зоны.

В процессе мониторинга используются средства наблюдения и сигнализации в режиме реального времени во всех случаях санкционированного и/или несанкционированного доступа. Используются автоматизированные средства, обеспечивающие выявление случаев несанкционированного доступа и инициирование действий по блокированию доступа. Компьютеры, серверы, другие терминалы доступа расположены в местах с ограниченным для посторонних лиц доступом.

Обеспечивается безопасность электрооборудования, используемого для поддержания функциональности информационных систем персональных данных, электрических кабелей, включая их защиту от повреждений и несанкционированного подключения. В случае возникновения исключительных, чрезвычайных или форс-мажорных обстоятельств обеспечена возможность отключения от электричества информационных систем персональных данных, включая возможность отключения любого компонента IT. Предусмотрены независимые источники электроснабжения краткосрочного действия, которые используются для надлежащего завершения рабочей сессии системы (компонента) в случае отключения от основного источника электрического питания. Предусматриваются и средства обеспечения пожарной безопасности в помещениях/офисах/кабинетах, где расположены информационные системы персональных данных и средства обработки персональных данных. Внедряются автоматические системы по обнаружению/сигнализации и тушению пожаров в помещениях/офисах/кабинетах, где расположены информационные системы персональных данных и средства обработки персональных данных.

Компьютеры, компьютерные терминалы и принтеры выключаются по окончании рабочих сессий. Средства обработки персональных данных, информация, которая содержит персональные данные или программное обеспечение, предназначенное для обработки персональных данных, выносятся из периметра безопасности только на основании соответствующего письменного разрешения руководства держателя персональных данных.

Факт выноса/вноса средств обработки персональных данных из/в периметр безопасности регистрируется.

Осуществляется идентификация и аутентификация пользователей информационных систем персональных данных и процессов, исполняемых от имени этих пользователей. Все пользователи (включая персонал технической поддержки, администраторов сети, системных программистов и администраторов базы данных) будут иметь уникальный идентификатор (пользовательский ID), который не должен содержать признаков уровня доступа пользователя.

Для подтверждения заявленной идентичности пользователя используются пароли, специальные физические устройства доступа с памятью (token) или микропроцессорные карты, биометрические методы аутентификации, основанные на индивидуальности и уникальности характеристик лица.

Администрирование идентификаторов пользователей включает:

1) однозначную идентификацию каждого пользователя;

2) проверку подлинности каждого пользователя;

3) получение авторизации от ответственного лица за выдачу идентификатора пользователя;

4) гарантирование того, что ID пользователя выдан конкретно определенному лицу;

5) дезактивацию учетной записи пользователя после заданного временного интервала неактивности (бездействия в течение не более 2 месяцев);

6) осуществление архивных копий ID пользователей.

Исходящая из системы информация, содержащая персональные данные, маркируется с указанием предписаний по дальнейшей обработке или распространению, в том числе с указанием единого идентификационного номера держателя персональных данных. Все методы удаленного доступа к информационным системам персональных данных защищены (с использованием VPN, криптирования, шифрования и др.), а также документируются, подвергаются мониторингу и контролю. Каждый используемый способ удаленного доступа к информационным системам персональных данных авторизуется ответственными лицами держателя персональных данных и разрешается только тем пользователям, которым это необходимо для выполнения установленных задач.

Беспроводной доступ к информационным системам персональных данных документируется, подвергается мониторингу и контролю. Беспроводной доступ к информационным системам персональных данных разрешен только при применении средств криптографической защиты

информации. Использование беспроводных технологий авторизуется ответственными лицами держателя персональных данных.

Обеспечивается невозможность доступа пользователей снаружи во внутреннюю сеть, в которой обрабатываются персональные данные.

Обеспечивается целостность передаваемых персональных данных с использованием средств криптографической защиты.

Обеспечивается защита от проникновения вредоносных программ в программное обеспечение, предназначенное для обработки персональных данных, – мера, которая обеспечивает своевременное автоматическое обновление средств, обеспечивающих защиту от вредоносного программного обеспечения и сигнатур вирусов. Обеспечивается централизованное администрирование механизмов защиты программного обеспечения для обработки персональных данных от вредоносных программ.

Держатели персональных данных проверяют регулярно, не менее одного раза в год, исполнение принятых технических и/или организационных мер для обнаружения неполадок по использованию телекоммуникационных систем при обработке персональных данных и/или внесения усовершенствования, в случае необходимости. Проверки безопасности осуществляются каждый раз, когда держатель персональных данных реорганизует или изменяет инфраструктуру.

В целях определения уровня защиты информационных систем персональных данных и предотвращения возможных случаев незаконного или случайного доступа к таким информационным системам, выявления слабых мест в механизмах их защиты Центр периодически проводит проверки безопасности, в том числе с осуществлением специальных технических мероприятий по имитации моделей доступа к информационным системам персональных данных. Результаты проведенных Центром проверок незамедлительно предоставляются держателю персональных данных, чей уровень защиты информационных систем персональных данных послужил объектом контроля, с предписанием, в случае необходимости, соответствующих мер, подлежащих принятию для обеспечения безопасности обработки персональных данных.

5. ПРАВА СООТВЕТСТВУЮЩИХ ЛИЦ

Согласно положениям Закона № 133 от 08.07.2011 г., субъект персональных данных пользуется следующими правами:

· Право на информирование (ст.12): это право лица получать от оператора, безвозмездно и по требованию, по запросу, подтверждение того, что касающиеся его данные обрабатываются или не обрабатываются ООО SC ”Totul pentru copii” SRL;

· Право на доступ к персональным данным (ст.13): любой субъект персональных данных имеет право получать от оператора, по запросу без задержки и безвозмездно любую касающуюся его информацию о персональных данных;

· Право на вмешательство в персональные данные (ст.14): любой субъект персональных данных имеет право получать от оператора, по запросу и безвозмездно, исправление, актуализацию, блокирование или удаление персональных данных, обработка которых противоречит вышеуказанному закону;

· Право на возражение субъекта персональных данных (ст.16): право субъекта высказывать в любое время, на обоснованном и законном основании, связанном с его частной ситуацией, возражение против того, чтобы касающиеся его персональные данные стали предметом обработки, кроме случаев, когда законом определено иное. Если возражение является обоснованным, выполняемая контролером обработка не может далее затрагивать эти данные;

· Право не отказаться под воздействием частного решения (ст.17): каждое лицо имеет право требовать полной или частичной отмены любого частного решения, порождающего юридические последствия в отношении его прав и свобод, и основанного исключительно на автоматизированной обработке персональных данных, предназначенной для оценки некоторых его личных аспектов, таких как профессиональная компетенция, надежность, поведение и т.п.;

· Право обращения в НЦОПД или судебную инстанцию (ст.18): любое лицо, которому нанесен ущерб в результате незаконно осуществленной обработки персональных данных или права и интересы которого, гарантированные настоящим законом, нарушены, вправе обратиться в суд с требованием компенсации за материальный и моральный ущерб.

Любая предоставленная вами информация будет считаться и являться вашим четким согласием с тем, чтобы ваши персональные данные использовались SC ”Totul pentru copii” SRL в соответствие с изложенными ниже целями.

Если вы желаете, чтобы ваши персональные данные были обновлены или удалены из базы данных, или у вас есть вопросы по поводу конфиденциальности данных, вы можете связаться с нами/уведомить нас в любой момент, используя размещенные на сайте контактные данные.

Если вы не желаете, чтобы ваши персональные данные собирались, просим не предоставлять их нам.

Также, для жалоб на несоблюдение прав, гарантированных Законом № 133 от 08.07.2011 г., соответствующее лицо может обратиться в Национальный центр по защите персональных данных РМ и/или в судебные инстанции.

6. ЦЕЛЬ СБОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

SC ”Totul pentru copii” SRL обрабатывает персональные данные своих клиентов и иных связывающихся или контактирующих с ним лиц, которые предоставляются путем открытия сайта www.baby-boom.md , в целях оформления и доставки приобретенных товаров.

Персональные данные (данные о личности, адрес, личный номерной код, номер телефона, возраст или любые иные подобные предоставленные данные) могут обрабатываться и использоваться SC ”Totul pentru copii” SRL, как в целях оформления и доставки товаров, заказанных с сайта предприятия, так и для составления баз данных и их использования при будущих обращениях и мероприятиях оператора, в соответствии с положениями Закона № 133 от 08.07.2011 г., о защите лиц при обработке персональных данных.

SC ”Totul pentru copii” SRL не разглашает третьей стороне никакие ваши данные (личные сведения или сведения по выбору) без вашего согласия, кроме случая, когда мы обоснованно убеждены, что этого от нас требует законодательство или что это необходимо для защиты прав или собственности нашего общества.

7. АУДИТ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

SC ”Totul pentru copii” SRL организует создание аудиторских записей безопасности в информационных системах персональных данных на случай следующих событий:

· Регистрируются попытки входа/выхода пользователя в систему (регистрируется дата и время попытки входа/выхода; ID пользователя; результат попытки входа/выхода – положительная или отрицательная);

· Регистрируются попытки получения доступа к приложениям и процессам, предназначенным для обработки персональных данных;

· Регистрируются попытки запуска/окончания рабочей сессии прикладных программ и процессов, предназначенных для обработки персональных данных, регистрируются изменения прав доступа пользователей и статус объектов доступа;

· Регистрируются изменения прав доступа (компетенции) пользователя и статуса объектов доступа;

· Осуществляется регистрация выхода из системы информации, содержащей персональные данные (электронных документов, данных и т.д.), регистрация изменений прав доступа субъектов и статус объектов доступа.

При нарушении аудита безопасности в информационных системах персональных данных или заполнения всего объема памяти, выделенного для хранения результатов аудита, информируется лицо, ответственное за политику безопасности персональных данных, и предпринимаются меры для восстановления работоспособности аудиторской системы.

Ведется постоянный мониторинг и анализ аудиторских записей безопасности в информационных системах персональных данных, в целях выявления необычных или подозрительных действий по использованию данных информационных систем, с составлением отчета о случаях выявления подобных действий, хранящихся в электронных вычислительных системах, и принятием мер, предусмотренных в политике безопасности для подобных случаев.

Результаты аудита безопасности в информационных системах персональных данных, представляющие собой операции по обработке персональных данных и средства проведения аудита, защищаются от несанкционированного доступа путем введения адекватных мер безопасности, в том числе, путем обеспечения их конфиденциальности и целостности.

Для обеспечения целостности информации, содержащей персональные данные, и информационных технологий, обеспечивается выявление, протоколирование и устранение неполадок компьютерных программ по обработке персональных данных, в том числе, установление исправлений и пакетов обновления этих компьютерных программ. Обеспечивается защита от проникновения вредоносных программ в программное обеспечение, предназначенное для обработки персональных данных, – мера, которая обеспечивает своевременное автоматическое обновление средств, обеспечивающих защиту от вредоносного программного обеспечения и сигнатур вирусов. Используются технологии и средства констатации вторжений, которые позволяют отслеживать происшествия в информационных системах персональных данных и констатировать атаки, в том числе те, которые обеспечивают выявление неавторизированных попыток использования информационных систем.

Для восстановления информации, содержащей персональные данные (для создания резервных копий), исходя из объема выполненной обработки, индивидуально, SC ”Totul pentru copii” SRLопределяет интервал времени, в котором выполняется резервное копирование информации, содержащей персональные данные и программное обеспечение для автоматизированной обработки персональных данных, но в любом случае этот период не может быть менее одного года, и которые хранятся в защищенных местах, вне зоны размещения этой информации и базового программного обеспечения. Процедуры по восстановлению резервных копий данных актуализируются и тестируются регулярно в целях обеспечения их эффективности.

SC ”Totul pentru copii” SRL проверяет регулярно, не менее одного раза в год, исполнение принятых технических и/или организационных мер для обнаружения неполадок в использовании телекоммуникационных систем в процессе обработки персональных данных и/или внесения усовершенствования, в случае необходимости. Проверки безопасности осуществляются каждый раз, когда держатель персональных данных реорганизует или изменяет инфраструктуру. В целях определения уровня защиты информационных систем персональных данных и предотвращения возможных случаев незаконного или случайного доступа к таким информационным системам, выявления слабых мест в механизмах их защиты Центр периодически проводит проверки безопасности, в том числе с осуществлением специальных технических мероприятий по имитации моделей доступа к информационным системам персональных данных.

8. УРЕГУЛИРОВАНИЕ ИНЦИДЕНТОВ С БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОЕННЫХ СИСТЕМ И ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Персонал, обеспечивающий эксплуатацию информационных систем персональных данных, проходит не реже одного раза в год инструктаж об ответственности и обязательствах в случае выполнения действий по управлению и реагированию на инциденты безопасности. Предусматривается механизм незамедлительного информирования руководства держателя персональных данных об инцидентах, связанных с нарушением безопасности информационных систем для персональных данных. Обработка инцидентов включает обнаружение, анализ, предотвращение развития, их устранение и восстановление безопасности. Используются автоматизированные средства для поддержания процесса обработки персональных данных и устранения инцидентов безопасности информационных систем персональных данных. Инциденты безопасности информационных систем персональных данных отслеживаются и документируются в постоянном режиме.

Исключаются бесконтрольное присутствие людей или транспортных средств и случайная установка антенн в зоне ближе 15 метров от расположения основных технических средств информационной системы персональных данных, в целях обеспечения безопасности обработки персональных данных. Помещения для серверов защищаются от утечки информации, содержащей персональные данные, в результате электромагнитной эмиссии посредством экранирования помещений или установки систем электромагнитных помех, которые проектируются, реализуются и исследуются специализированными отраслевыми предприятиями. Исключается или ограничивается неавторизированная установка других электрических приборов, радио и других видов в помещениях, где расположены технические средства обработки персональных данных, с целью обеспечения безопасности обработки персональных данных. Оборудование, габариты которого выступают за пределы контролируемого периметра, устанавливается на расстоянии не менее 3 метров от ресурсов IT, в которых обрабатываются персональные данные.