**ПОЛИТИКА БЕЗОПАСНОСТИ В СФЕРЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ SRL «NEW POST INTERNATIONAL MLD»**

Настоящая Политика по обработке персональных данных (здесь и далее – «**Политика**») была разработана и одобрена SRL «NEW POST INTERNATIONAL MLD», IDNO 1014600029674 с юридическим адресом: бул. Штефан чел Маре, 65, оф. 806, мун. Кишинэу, Республика Молдова (здесь и далее, – «**Контролер**»), компанией, которая существует и функционирует в соответствии с законодательством Республики Молдова в соответствии с положениями *Закона № 2020133 от 8 июля 2011 г. О защите персональных данных* и требований к крипто обработке и обеспечению безопасности персональных данных при их обработке в рамках информационных систем персональных данных, утвержденных Постановлением Правительства № 1123 от 14 декабря 2010 г., а также в соответствии с положениями других регулирующих предписаний, касающихся защиты персональных данных субъекта данных, в отношении следующего:

## 1. СФЕРА ПРИМЕНЕНИЯ

1. Эта Политика представляет собой документ внутреннего распорядка, который является обязательным для исполнения Контролером, его сотрудниками и контрагентами Контролера. Контролер обеспечит выполнение этой Политики посредством доведения ее содержания до сведения всех своих сотрудников. Содержание данной Политики будет доведено до сведения Клиентов Контролера путем ее публикации на веб-портале www.novaposhta.md.
2. Настоящая политика применяется и является обязательной для всей операционной деятельности компании, связанной с обработкой персональных данных, но без ограничения: обработка данных о сотрудниках, обработка данных о Клиентах/поставщиках/субподрядчиках; обработка данных средствами видеонаблюдения и обработка данных в ходе ведения бухгалтерского учета.

3. Сотрудники и контрагенты Контролера будут обрабатывать персональные данные с соблюдением принципов и правил, установленных в настоящей Политике, в законных целях.

## 2. ЦЕЛЬ

1. Цель разработки настоящей Политики – определить требования к защите и порядок защиты персональных данных от несанкционированных утечек, к соблюдению правил обработки персональных данных, обеспечению защиты частной жизни субъектов персональных данных.

2. Система бухгалтерского учета и начисления баллов, данные о сотрудниках, клиентах и поставщиках, а также любые другие данные, обработанные в соответствии с настоящей Политикой, хранятся на серверах Контролера. Данные **передаются трансгранично** в Украину компании ООО Нова Пошта (New Post S.R.L.) на основании заключенного договора о передаче.

3. Данные, обрабатываемые в рамках этой системы, хранятся на серверах Контролера для хранения на серверах, расположенных по зарегистрированному адресу импортера данных, для реализации целей хранения и извлечения данных в результате сбора информации, полученной в рамках заключения договоров с клиентами, а также для статистических целей. Данные хранятся на серверах столько, сколько необходимо в соответствии с заключенным договором. В случае, если договор о трансграничной передаче данных расторгается, приостанавливается или иным способом нарушается возможность хранения данных экспортером данных вне пределов юрисдикции Республики Молдова, Контролер временно приостановит передачу данных. В любом случае, за сторонами соглашения о трансграничной передаче сохраняются их права и обязанности в отношении передаваемых персональных данных. Данные **передаются трансгранично** в Украину.
4. Персональные данные, зарегистрированные в настоящей системе учета, будут храниться на серверах Контролера, находящиеся вне пределов Республики Молдова. В этой связи Контролер заключил с уполномоченным зарубежным Контролером Соглашение о трансграничной передаче персональных данных, которое детально регламентирует условия и детали передачи персональных данных, регулируя права и обязанности импортера и экспортера данных. В частности, импортер данных обязан обрабатывать персональные данные только на условиях и в соответствии с инструкциями экспортера данных.

5. **Трансграничной передаче будут подлежать следующие категории персональных данных:** Персональные данные относятся к следующим категориям данных: имя, фамилия и отчество; пол, подпись, электронная подпись, государственный персональный идентификационный номер (IDNP); дата и место рождения; гражданство, данные актов гражданского состояния, персональный код медицинского страхования (CPAM), мобильный телефон, адрес места проживания / пребывания, телефон/ факс, адрес электронной почты, профессия, должность, профессиональная подготовка,– дипломы – образование, семейное положение, сведения о членах семьи экономическое или финансовое положение, размер зарплаты брутто, премии, бонусы, надбавки, поощрения, данные о больничных листах, банковские реквизиты, изображение (фотография), водительские права, данные о дисциплинарных взысканиях, персональный код социального страхования (CPAS), персональных код медицинского страхования, данные из регистрационных свидетельств, место работы.
6. Субъект персональных данных будет проинформирован о передаче данных, а также о его правах. Трансграничная передача данных осуществляется только при условии явным образом выраженного согласия субъекта персональных данных. Согласие на трансграничную передачу данных будет включено в Индивидуальный трудовой договор в форме явно выраженного согласия. Образец формулировки согласия на трансграничную передачу данных прилагается к настоящей Политике. Почтовый счет-фактура (накладная), посредством которого обрабатываются данные Клиентов, прилагается к настоящей Политике.

7. Как экспортер данных, так и импортер данных обеспечат строгое соблюдение прав субъекта данных. В этом ключе, субъектам данных напрямую или через третью сторону будет предоставляться личная информация о них, если она имеется у организации, за исключением запросов, которые являются явно неправомочными. Источники персональных данных не должны быть идентифицированы, когда этого невозможно достичь ценой разумно обоснованных усилий, и в случае, если помимо прав субъекта персональных данных, были нарушены права других лиц. Субъекты данных должны иметь возможность получить исправление личной информации о них, с последующими изменениями, или удалить ее, если она является неточной или обрабатывается вопреки этим принципам. Если имеются какие-либо веские причины для сомнений в легитимности заявки, организация может потребовать дополнительных обоснований, прежде чем приступить к исправлению, изменению или удалению данных. Уведомление о любых исправлениях, изменениях или удалении, осуществленных третьими лицами, которым были раскрыты данные, не является обязательным в случае, если исполнение такового уведомления требует непропорциональных усилий. Физическое лицо также должно иметь возможность возражать против обработки относящихся к нему персональных данных, если имеются законные основания, связанные с его личными обстоятельствами. Бремя доказывания любого отказа возлагается на импортера данных, и субъект данных всегда может оспорить отказ перед органами государственного управления.

## 3. КАТЕГОРИИ СУБЪЕКТОВ ДАННЫХ И КАТЕГОРИИ ДАННЫХ

**1.** Контролер в связи со своей деятельностью обрабатывает персональные данные своих сотрудников (состоящих в штате на текущий момент, кандидатов на замещение вакантных должностей), а также данные, относящиеся к физическим лицам: партнерам, субподрядчикам и другим поставщикам товаров и услуг Контролера в пределах, установленных законодательством («**Субъекты**»).

**2.** Категории персональных данных, обрабатываемых Контролером, приведены в Приложении 1 к настоящей Политике.

**3.** Контролер обрабатывает персональные с использованием ручных и/или автоматических средств, с соблюдением правовых требований и в условиях, обеспечивающих безопасность, конфиденциальность и соблюдение прав субъектов данных.

## 4. ОБЩИЕ ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Персональные данные обрабатываются:

*a) корректно и в соответствии с положениями законодательства* – обработка персональных данных будет осуществляться в строгом соответствии с законодательством в области защиты персональных данных. Этот факт предполагает, что перед сбором, использованием и раскрытием персональных данных обработка должна быть явным образом обоснована наличием правовых оснований или правовых обязательств;

b) *в определенных, явных и законных целях и не обрабатываются далее в несовместимых целях* – любая обработка персональных данных осуществляется в целях, которые являются четко определенными, явными и законными, адекватными, актуальными и не чрезмерными по отношению к целям, для которых они собираются и в последующем обрабатываются. Собранная информация предназначена для использования Контролером и его партнерами в законных целях и может быть раскрыта, при необходимости, следующим получателям: сторонам, заключившим договор, государственным нотариусам, судам, юридическим и финансовым консультантам, включая адвокатов, поставщикам товаров и услуг, государственным учреждениям, банковским учреждениям, государственным реестрам и другим типам получателей, которых это непосредственно касается.

c) *с соблюдением конфиденциальности* – работники Контролера, обученные непосредственной обработке персональных данных, обязаны соблюдать конфиденциальность персональных данных, обрабатываемых Контролером, согласно положениям соответствующего закона и / или договоров.

d) *с согласия субъекта персональных данных* – любая обработка персональных данных субъектов может осуществляться только в том случае, если они выразили явное согласие на такую обработку, за исключением случаев, предусмотренных действующим законодательством.

e) *с обеспечением защиты субъектов персональных данных* - субъекты персональных данных имеют право на доступ к данным о них, которые обрабатываются Контролером, на вмешательство и возражения в их отношении, право не оказаться под воздействием частного решения, а также право обращаться в Национальный Центр защиты персональных данных или в суд для защиты любых

прав, гарантированных законом, которые были по отношению к ним нарушены. Ограничение этих прав может быть допущено в случаях, предусмотренных законом.

f) *с обеспечением безопасности* – меры обеспечения безопасности персональных данных устанавливаются таким образом, чтобы обеспечить адекватный уровень безопасности персональных данных, обрабатываемых Контролером.

g) *адекватно, релевантно и не избыточно* – любая обработка персональных данных должна соответствовать цели, для которой они были собраны, и быть релевантной и не избыточной в контексте преследуемой цели. В целях соблюдения этих требований контролер применяет принцип минимизации персональных данных, который заключается в сборе только тех сведений, которые строго необходимы для реализации предоставляемых услуг. Оценка соблюдения этих требований будет проводиться на периодической основе и в случае необходимости.

h) *с соблюдением точности и актуальности* – категории данных, обрабатываемых контролером, устанавливаются исчерпывающе, обрабатываются только подтвержденные данные. Контролер периодически проверяет обработанные персональные данные, противопоставляя обработанные данные тем, которые принадлежат субъектам персональных данных.

i) *в течение периода, который не будет превышать продолжительность, необходимую для достижения целей, для реализации которых данные были собраны и впоследствии обработаны* – персональные данные хранятся только в период существования гражданских отношений и / или в течение срока, установленного специфическим законодательством, в соответствии с которым обрабатываются персональные данные.

## 5. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. В случае, если персональные данные являются предоставленными непосредственно субъектом данных, в соответствии с положениями ст. 12 Закона о защите персональных данных, субъекту персональных данных необходимо предоставить следующую информацию, за исключением тех случаев, когда он уже обладает ею:

a) личность контролера или, в зависимости от обстоятельств, лица, уполномоченного контролером (обработчика) *(наименование, юридический адрес, идентификатор IDNO, регистрационный номер в Реестре учета контролеров персональных данных);*
b) в отношении конкретной цели обработки собранных персональных данных;
c) в отношении получателей или категорий получателей персональных данных;
d) наличие прав на информирование и доступ к собранным данным; прав на вмешательство *(в частности, исправление, обновление, блокировку или удаление персональных данных, обработка которых противоречит закону, в частности, в связи с неполным или неточным характером данных)* и возражение, а также условий, при которых эти права могут быть реализованы; указание, являются ли ответы на вопросы, с помощью которых собираются данные, обязательными или добровольными, включая возможные последствия отказа отказа ответа на вопросы, посредством которых собирается информация.

2. Субъектам персональных данных обеспечивается право доступа и возможность ознакомления с оформленными документами с целью проверки правильности их составления, оспаривания неубедительности или неправильного включения некоторых данных, а также других ошибок, допущенных при регистрации данных о них. В связи с этим лица, ответственные за обработку персональных данных, обеспечат доступ субъекта персональных данных только к тем данным, которые непосредственно к нему относятся, с исключением возможности консультирования персональнных данных, относящихся к другим субъектам персональных данных, содержащихся в персональных карточках *(других материалах),* за исключением случаев, когда подающие соответствующий запрос лица реализуют законный интерес, не сопряженный с ущербом интересам или основным правам и свободам субъекта персональных данных.

3. Право на информирование обеспечивает контролер персональных данных *(или организация, обеспечивающая обслуживание системы и / или предоставляющая аутсорсинговые услуги контролера )* всем лицам, чьи персональные данные подлежат обработке.

4. В случае реализации субъектом персональных данных права на вмешательство неточные данные будут обновляться путем исправления или удаления, в качестве основания достоверности могут служить только законные источники *(удостоверения личности, документы записи актов гражданского состояния, основные государственные информационные ресурсы и т. д.),* изменение будет внесено во все управляемые информационные системы и системы учета.

## 6. ПРИМЕНЕНИЕ, КОМПЕТЕНЦИЯ И АДРЕСАТЫ ПОЛИТИКИ

1. Настоящая Политика применяется и является обязательной для всей операционной деятельности Компании, доводится до сведения сотрудников и партнеров Контролера, и является для них обязательной для исполнения.

Ответственное лицо

2. Контролер приказом, подписанным лицом, занимающим руководящую должность, назначит из числа своих работников лицо, ответственное за разработку, внедрение и мониторинг выполнения обязательств в области защиты персональных данных. Лицом, ответственным за защиту персональных данных, является юрисконсульт Компании («**Ответственное лицо**»).

3. Обязанности ответственного лица:

a) проводит анализ рисков, связанных с информационными ресурсами;
b) предусматривает меры логической защиты;
c) обеспечивает проверку наличия, обновления и достаточности лицензий на информационные ресурсы;
d) обеспечивает учет аудита компьютерных систем, а также их хранение и доступность для проверки в соответствии с правилами внутреннего распорядка;
e) определяет процедуру, с помощью которой пользователи информационной системы получают право доступа к информационным ресурсам и управления ими, а также организует контроль использования этих ресурсов;
f) обеспечивает создание резервных копий информационных ресурсов и их хранение, а также реконструкцию информационных ресурсов в случае нарушения работы информационных ресурсов или невозможности работы из-за повреждения технических ресурсов или по другим причинам;
g) предусматривает меры физической защиты;
h) участвует в анализе рисков, выявляет угрозы для информационной системы в отношении технических ресурсов и оценивает вероятность этих угроз;
i) обеспечивает восстановление технических ресурсов в случае их повреждения.

4. Ответственное лицо должно обеспечить введение соответствующих процедур обработки данных, а также ведение протоколов слушаний для регистрации актов управления Персональными данными.

5. Лицо, ответственное за защиту Персональных данных, обеспечивает обучение сотрудников, а также тестирование их знаний в сфере защиты персональных данных.

6. Ответственное лицо будет принимать своевременное и адекватное участие во всех аспектах процесса защиты персональных данных.
7. Контролер обеспечивает поддержку ответственного лица в выполнении его задач, обеспечивает ресурсы, необходимые для того, чтобы специалист по защите персональных данных мог выполнять описанные выше задачи, и предоставляет доступ к Персональным данным и документам обработки Персональных данных, а также возможность обновления специальных знаний специалисту по защите данных.

8. Задачи ответственного лица в сфере защиты персональных данных:

a) информировать и консультировать сотрудников, осуществляющих обработку Персональных данных, в отношении их полномочий в соответствии с документами внутреннего распорядка Контролера и нормативных регулирующих актов по защите Персональных данных;
b) контролировать соблюдение внутренних и внешних нормативных актов по защите Персональных данных, включая разделение задач, информировать и обучать сотрудников, принимающих участие в действиях по обработке персональных данных;
c) по запросу консультировать по вопросам Оценки воздействия на защиту Персональных данных, участвовать в подготовке этой оценки и осуществлять надзор за ее проведением;
d) разработать и последовательно вести Журнал регистрации нарушений в области защиты Персональных данных;
e) сотрудничать с компетентным Надзорным органом и выступать в роли контактного лица при взаимодействии с Надзорным органом по вопросам, связанным с обработкой Персональных данных, в том числе касающимся предварительных обсуждений и других аспектов;
f) консультировать Заинтересованных лиц (Субъектов данных), которые обратились к специалисту по защите персональных данных по поводу обработки Персональных данных в Компании.

9. Права ответственного лица в сфере защиты персональных данных:

a) собирать информацию для определения процессов обработки Персональных данных, анализировать и проверять соответствие обработки Персональных

данных требованиям актов внутреннего распорядка, а также информировать, консультировать и давать рекомендации в отношении обработки Персональных данных;

b) проводить аудит обработки Персональных данных без предварительного уведомления;

c) знакомиться с документами компании, техническими и организационными требованиями, влияющими на обработку Персональных данных, а также своевременно получать информацию об инцидентах в области информационной безопасности и знакомиться с записями в Журнале регистрации инцидентов в области информационной безопасности;

d) принимать участие в принятии резолюций, целью которых является защита Персональных данных, ознакомиться с соответствующими документами, чтобы высказать свое мнение и предоставить соответствующие рекомендации по этому поводу.

## 7. КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

a) Контролер осознает важность и значимость информационной безопасности и определяет компоненты информационной безопасности и требования, которым сотрудники Контролера должны соответствовать в повседневной трудовой деятельности.

b) Безопасность данных описывается их конфиденциальностью, целостностью и доступностью. Компания следит за тем, чтобы выполнялись следующие требования:

- информация должна быть доступна только лицам, имеющим право на ее получение (конфиденциальность);
- данные и методы обработки являются точными и полными (целостность);
- авторизованные пользователи должны иметь доступ к информации в случае необходимости (доступность).

c) Компания реализует техническую защиту Персональных данных с использованием физических и логических средств защиты, обеспечивая защиту от угрозы безопасности Персональных данных, вызванной физическим воздействием, и защиту, осуществляемую средствами информационных технологий (средствами ИТ). При выборе типа хранения Персональных данных будет учитываться возможность повреждения в результате пожара, наводнения, взрыва, а также других инцидентов безопасности, вызванных природой, ИТ и людьми.

d) Технические ресурсы, содержащие Персональные данные, включая настольные и переносные компьютеры, жесткие диски, когда они не используются, хранятся в местах, недоступных для других людей (например, в запертых на ключ комнатах или шкафах).

## 8. КЛАССИФИКАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ИХ УРОВНЮ, ЦЕННОСТИ И КОНФИДЕНЦИАЛЬНОСТИ, РЕГИСТР ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В рамках своей деятельности Контролер ведет учет целого ряда персональных данных, таких как учет сотрудников, преподавателей, участников тренинга, партнеров Контролера, бухгалтерский учет, учет посетителей и т. д., записывая их в соответствующие журналы учета. Во всех этих журналах учета содержатся персональные данные. Все записи, содержащие персональные данные, должны храниться в защищенных местах в строгом соответствии с настоящими правилами и использоваться только в тех целях, для которых они созданы.

8.2. Журналы учета

a) Контролер составляет и ведет Журнал учета, который регулярно пересматривается и заполняется в соответствии с фактической обработкой персональных данных, включая периодические пересмотры сроков хранения персональных данных, определенных в журнале учета.

b) Журнал учета ведется с целью общей регистрации актов, совершенных с использованием персональных данных, в рамках одной или нескольких целей, включая регистрацию и контроль получателей Персональных данных.

c) В случае необходимости Контролер предоставляет доступ к реестру компетентному Надзорному органу.

## 9. ПРАВИЛА И ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

1. Доступ в помещения:

1.1. Руководство Контролера осознает важность и значимость информационной безопасности и определяет компоненты информационной безопасности и требования, которым сотрудники Контролера должны соответствовать в повседневной трудовой деятельности.

1.2. Доступ в рабочие помещения / офисы Контролера, или в помещения, где расположены информационные системы персональных данных, обрабатываемые Контролером, ограничен, осуществляется на основе идентификационных бейджей или карт или ключей доступа, и разрешен только сотрудникам Контролера, партнерам и авторизованным посетителям (категория «**Пользователи**»). Доступ посетителей регистрируется в журналах учета, которые хранятся не менее одного года. По истечении срока хранения журналы учета ликвидируются, а данные и документы, содержащиеся в журнале учета, подлежащем ликвидации, передаются в архив. Перед предоставлением физического доступа к информационным системам персональных данных выполняется проверка компетенций доступа.

1.3. Осуществляется администрирование и мониторинг физического доступа во всех точках доступа к информационным системам персональных данных, в том числе реализуется реагирование на нарушение режима доступа. Журналы учета хранятся минимум один год, по истечении которого они ликвидируются, а данные и документы, содержащиеся в журнале учета, подлежащем ликвидации, передаются в архив.

1.4. Компьютеры, серверы, другие терминалы доступа размещаются в местах с ограниченным доступом для посторонних.

2. Управление учетными записями доступа (аккаунтами)

2.1. Управление учетными записями доступа пользователей, которые обрабатывают персональные данные, включая их создание, активацию, изменение, проверку, деактивацию и удаление, осуществляется Контролером. При администрировании используются автоматизированные средства поддержки. Действие учетных записей доступа временных пользователей, которые обрабатывают персональные данные, автоматически прекращается по истечении установленного периода времени (для каждого типа учетной записи доступа в отдельности). Автоматически отключаются, по истечении трех месяцев, учетные записи доступа неактивных пользователей, производящих обработку персональных данных. Используются автоматизированные средства регистрации и информирования о создании, изменении, деактивации и прекращении действия учетных записей доступа.

2.2. В конференц-залах, предназначенных для общественности, в меру возможностей будет сведена к минимуму деятельность по обработке персональных данных, а средства и оборудование, обеспечивающие доступ к данным, обрабатываемым Контролером, будут защищены.

2.3. Компьютеры, серверы, другие терминалы доступа размещаются в местах с ограниченным доступом для посторонних.

3. Целостность периметра

3.1. Периметр офиса Контролера определен конкретно и четко. Периметр здания или помещения, где расположены средства обработки персональных данных, должен быть физически целостным. Наружные стены помещений должны быть прочными, входы оснащены замками.

4. Меры по защите технических ресурсов от чрезвычайных ситуаций (пожары, наводнения) :

4.1. Для обеспечения защиты центра обработки данных была построена современная система пожаротушения. Надзор за состоянием пожарной безопасности в центре обработки данных осуществляется Администратором.

4.2. Компьютер, на котором хранится информация с определенной степенью конфиденциальности, не может быть подключен к внешним сетям локальной сети, из которой возможен доступ к внешним сетям.

4.3. Информация о специальном уровне конфиденциальности не передается через внешние сети.

4.4. Если компьютеры, содержащие информацию с определенным уровнем конфиденциальности, подключены к локальной сети, кабели локальной сети не должны пересекать территорию, где не предусмотрена соответствующая физическая защита от угрозы компьютерной системе, а сетевые устройства должны быть расположены в помещениях с соответствующей физической защитой от угрозы компьютерной системе.

4.5. Защита данных клиентов от несанкционированного доступа обеспечивается: системами сигнализации и системами слежения высокого уровня, работающими в режиме 24/7.

5. Аудит безопасности

5.1. Запись попыток входа пользователя в систему / выхода пользователя из системы определяется по следующим параметрам:

а) дата и время попытки входа / выхода;
б) идентификатор ID пользователя;
в) результат попытки входа в систему / выхода из системы – положительный или отрицательный.

5.2. Также осуществляется регистрация попыток начала/завершения рабочих сессий прикладных программ и процессов, предназначенных для обработки персональных данных, регистрация изменений прав доступа пользователей и состояния объектов доступа по следующим параметрам:

a) дата и время попытки запуска;
b) наименование / идентификатор прикладной программы или процесса;
c) идентификатор ID пользователя;
d) результат попытки запуска – положительный или отрицательный.

5.3. Осуществляется регистрация попыток получения доступа (выполнения операций) для приложений и процессов, предназначенных для обработки персональных данных, по следующим параметрам:

a) дата и время попытки получения доступа (выполнения операции);
b) наименование (идентификатор) прикладной программы или процесса;
c) идентификатор ID пользователя;
d) спецификации защищенного ресурса (идентификатор, логическое имя, имя файла, номер и т. д.);
e) тип запрошенной операции (чтение, запись, удаление и т.д.);
f) результат попытки получения доступа (выполнения операции) - положительный или отрицательный.

5.4. Производится регистрация изменений прав доступа (полномочий) пользователя и статуса объектов доступа по следующим параметрам:
a) дата и время изменения полномочий;
b) идентификатор ID администратора, который внес изменения;

c) идентификатор ID пользователя и его полномочия или указание объектов доступа и их новый статус.

5.5. Осуществляется регистрация выхода из информационной системы, содержащей персональные данные (электронные документы, данные и т.д.), регистрация изменений прав доступа субъектов и статуса объектов доступа по следующим параметрам:

a) дата и время выдачи;
b) наименование информации и пути доступа к ней;
c) спецификация оборудования (устройства), выдавшего информацию (логическое имя);
d) идентификатор ID пользователя, который запросил информацию;
e) объем выданного документа (количество страниц, файлов, копий) и результат выдачи - положительный или отрицательный.

6. Хранение данных аудита

6.1. Осуществляется постоянный мониторинг и анализ записей аудита безопасности в информационных системах персональных данных с целью выявления необычных или подозрительных действий при использовании этих информационных систем, с предоставлением отчетов о случаях выявления таких действий. Срок хранения результатов аудита безопасности в информационных системах персональных данных составляет 2 года, с тем чтобы их можно было использовать в качестве доказательств в случае инцидентов безопасности, возможных расследований или судебных процессов.

7. Антивирусная защита

7.1. Контролер и работники обеспечат защиту от проникновения вредоносных программ (вирусов) в программы, предназначенные для обработки персональных данных, что обеспечивает возможность автоматического и своевременного обновления средств обеспечения защиты от вредоносных программ. В то же время Контролер и его сотрудники будут использовать технологии и средства обнаружения вторжений, которые позволяют отслеживать события в информационных системах персональных данных и обнаруживать атаки, в том числе и те технологии и средства, которые обеспечивают выявление попыток несанкционированного использования информационных систем. Обеспечивается выявление, регистрация и устранение недостатков программных средств, предназначенных для обработки персональных данных, включая установку

исправлений и пакетов обновления этих программных средств. Осуществляется контроль и учет установки и удаления программного обеспечения, технических и программно-технических ресурсов, используемых в информационных системах персональных данных. Программное обеспечение, предназначенное для обработки персональных данных и информации, содержащей персональные данные, доступ к которым осуществляется через системы общественного доступа, защищается методом использования цифровой/мобильной подписи.

8. Резервные копии

8.1. Раз в год Контролер будет обеспечивать создание резервных копий информации, содержащей персональные данные, и программных копий, используемых для автоматизированной обработки персональных данных. Резервные копии хранятся в защищенных местах за пределами зоны размещения этой информации. Резервные копии тестируются с целью проверки безопасности носителей информации и целостности информации, содержащей персональные данные. Процедуры восстановления резервных копий регулярно обновляются и проверяются в целях обеспечения их эффективности.

9. Внутренние проверки

9.1. Не реже одного раза в год проверяется выполнение технических и/или организационных мер, принятых для выявления сбоев в использовании телекоммуникационных систем при обработке персональных данных и/или для внесения улучшений в случае необходимости. Проверки безопасности каждый раз обновляются. В зависимости от результатов проверки Контролер персональных данных принимает меры по реорганизации процессов или меняет инфраструктуру.

10. Целостность оборудования

10.1. Оператор и его сотрудники должны обеспечить безопасность электрооборудования, используемого для поддержания работоспособности информационных систем персональных данных, электрических кабелей, маршрутизаторов, коммутаторов, включая их защиту от повреждений и несанкционированных подключений. Сетевые кабели, посредством которых осуществляются операции по обработке персональных данных, должны быть защищены от несанкционированных подключений или повреждений.

10.2. Аварийное отключение происходит в случае исключительных ситуаций, поломок или форс-мажорных обстоятельств, должна быть обеспечена возможность отключения энергоснабжения информационных систем персональных данных, включая возможность отключения любого компонента информационных технологий.

10.3. Сотрудники Контролера должны по окончанию рабочих сессий выключать компьютеры, терминалы доступа и принтеры.

10.4. Использование ИБП (UPS): Контролер предоставит источники бесперебойного питания кратковременного действия, используемые для правильного завершения рабочего сеанса системы (компонента) в случае отключения от основного источника энергоснабжения.

## 10. ДОСТУП И ПАРОЛИ

1. Пароли

10.1. Контролер и его сотрудники должны соблюдать следующие правила обеспечения информационной безопасности в случае выбора и использования паролей:

a) сохранение конфиденциальности паролей;
b) запрещается записывать пароли на бумажном носителе, если безопасность их хранения не обеспечена, пароли хранятся в зашифрованном виде с использованием одностороннего криптографического алгоритма (хеш-функции);
c) изменение паролей один раз в 3 месяца и каждый раз, когда присутствуют признаки возможного взлома системы или пароля;
d) выбор качественных паролей размером не менее 8 символов, не связанных с персональными данными пользователя, не содержащих последовательных идентичных символов и не состоящих полностью из групп цифр или букв;
e) отключение автоматизированного процесса регистрации пароля (с использованием сохраненных паролей);

f) пользователям предоставляется возможность выбирать и изменять отдельные пароли, в том числе активировать процедуру процедуру учета ошибочных вводов паролей;
g) доступ блокируется после трех неправильных попыток входа в систему;
h) на момент ввода пароли не отображаются в явном виде на мониторе;
i) после установки системы меняется информация для входа в систему, используемая в стандартной комплектации;
j) обеспечивается хранение истории хэшей предыдущих паролей пользователей (в течение одного года) и предотвращение их повторного использования.

10.2. Если договор, регулирующий отношения между Контролером и пользователем, был расторгнут, приостановлен или изменен, а новые задачи не требуют доступа к персональным данным, либо права доступа пользователя были изменены, либо пользователь злоупотреблял полученными кодами с целью совершения неправомочных действий, отсутствовал в течение длительного периода, идентификационные коды и коды аутентификации отменяются или их действие приостанавливается. Неактивная учетная запись пользователя (бездействие в течение максимум 2 месяцев) деактивируется;

10.3. Доступ к функциям безопасности информационных систем персональных данных и к их данным предоставляется только ответственному лицу.

10.4. Пользователи информационных систем персональных данных наделяются только теми правами / полномочиями, которые необходимы для достижения поставленных перед ними целей. Права доступа пользователей к информационным системам персональных данных регулярно пересматриваются, чтобы гарантировать отсутствие несанкционированного доступа (максимум каждые шесть месяцев) и после любого изменения статуса пользователя. Доступ к информации и ресурсам предоставляется на основе принципа „необходимости доступа к информации". Системы разработаны с необходимым минимумом информации для осуществления деятельности. Пользователям предоставляется самый низкий уровень доступа, необходимый для выполнения их должностных обязанностей.

10.5. Защита удаленного доступа: Все методы удаленного доступа к информационным системам персональных данных Контролера защищены посредством использования VPN, шифрования, кодирования и других методов защиты, также они документируются и подлежат мониторингу и контролю со стороны Контролера. Каждый способ удаленного доступа к информационным системам персональных

данных должен быть санкционирован руководителем Контролера и/или ответственным лицом Контролера, назначенным руководителем в соответствии с настоящей Политикой, и разрешен только Пользователям, которым такой доступ необходим для выполнения поставленных профессиональных задач.

10.6. Доступ к электронным устройствам (мобильные телефоны, планшеты, ноутбуки и т.д.): Использование портативного и мобильного оборудования, обеспечивающего доступ к информационным системам персональных данных Контролера, должно быть разрешено руководителем Контролера или ответственным лицом, назначенным руководителем.

## 11. ДОСТУП К СЕТИ ИНТЕРНЕТ И ЭЛЕКТРОННОЙ ПОЧТЕ

1. Системы электронной почты и сети Интернет являются быстрыми и эффективными средствами коммуникации и сбора информации. Оба типа связи принадлежат Контролеру и предоставляются в распоряжение его работникам в качестве эффективных средств связи и информирования, которые будут использоваться в ходе осуществления профессиональной деятельности и для достижения ее целей. Беспроводные Интернет-сети (wi-fi), управляемые Контролером, защищены паролем. Доступ к этому паролю может быть предоставлен руководителем Контролера.

2. В целях обеспечения безопасности компьютерной сети, а также для предотвращения ненадлежащего использования доступа в Интернет, ряд данных трафика автоматически и непрерывно сохраняется (без вмешательства человека) для любого компьютера, входящего в состав локальной сети Контролера. Как правило, эта информация хранится в течение нескольких недель или месяцев, после чего удаляются окончательно путем перезаписи. Данные о трафике с целью наблюдения за сотрудниками Контролера не сохраняются. Тем не менее, Контролер может анализировать существующие в определенный момент записи о конкретном работнике, проинформировав посетителя о такой проверке и об ее причинах.

3. Внимание к вложениям. Электронные письма являются основным средством, с помощью которого вирусы могут быть внедрены в локальную сеть, поэтому весь рабочий коллектив, а также любой человек, который получит доступ к информационным ресурсам Контролера, должен проявлять осторожность при открытии вложений, особенно если их происхождение неясно / небезопасно / подозрительно или файл, помещенный во вложение, имеет расширение .exe.

4. О личных сообщениях. Электронные сообщения и прилагаемые к ним документы, используемые работниками Контролера для служебной коммуникации, не классифицируются как личные, если для их создания / хранения используется служебный компбютер. Резервная копия всех писем, отправленных со служебных адресов электронной почты, или полученных на служебные адреса электронной почты хранится, как правило, на сервере Контролера.

5. О бесплатных серверах электронной почты. Интернет предлагает множество вариантов бесплатной электронной связи, например @gmail.com, @yahoo.com, @mail.ru и т. д. Контролер предупреждает, что эти системы электронной связи не соответствуют требованиям защиты персональных данных. Работники Контролера будут воздерживаться от передачи персональных данных Субъектов данных с использованием таких систем связи. Контролер гарантирует, что у него создана система корпоративной электронной связи, которая защищена в строгом соответствии с настоящими правилами и Законом О защите персональных данных.

## 12. ПОРЯДОК ХРАНЕНИЯ И УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, НОСИТЕЛЕЙ ИНФОРМАЦИИ

12.1. Информационные носители в центре обработки данных, где хранятся данные Субъектов данных, которые были повреждены или изношены, должны храниться в безопасном месте в центре обработки данных после их отключения от программного обеспечения центра обработки данных.

12.2. Данные Субъектов данных подлежат уничтожению, когда срок их хранения определяется в соответствии с действующим законодательством, правилами внутреннего распорядка Контролера и указывается в разделе "срок хранения" в Журнале учета.

12.3. Хранение персональных данных осуществляется в виде электронных файлов и на бумажных носителях. Электронные и бумажные файлы, содержащие персональные данные, хранятся в течение срока, указанного в Журнале учета.

12.4. Доступ в помещения/периметр, где расположены информационные системы и системы учета персональных данных, ограничен и разрешен только лицам, имеющим необходимую авторизацию в соответствии с

институциональной политикой безопасности /утвержденными ведомственными предписаниями.

12.5. Накопление и хранение персональных данных (в электронном формате), структурированных в системах учета, в компьютерах, подключенных к интернету, не оборудованных специальными техническими и программными средствами защиты и не имеющими установленных лицензированных программ, антивирусных программ, систем контроля безопасности программного обеспечения, обеспечения периодического выполнения резервного копирования и аудита, – запрещено.

12.6. Введение в периметр институциональной безопасности и использование персональных компьютеров или носителей информации в служебных целях запрещено. Кроме того, доступ к компьютерам на территории компании защищен/ограничен посредством создания профилей пользователей, а права администратора предоставляются только лицу, ответственному за реализацию политики безопасности, действующей в Компании.

12.7. Хранение персональных данных на магнитном, оптическом, лазерном, бумажном или другом носителе информации, на котором создается, фиксируется, передается, принимается, хранится или иным образом используется документ и который позволяет его воспроизводить, обеспечивается путем помещения их в сейфы или запирающиеся на ключ шкафы. Несанкционированное перемещение носителей информации с персональными данными за пределы периметра безопасности Контролера запрещен.

12.8. Компания пересматривает условия хранения Персональных данных, определенные реестром, по мере необходимости, однако не реже одного раза в 2 (два) года.

12.9. В ходе оценки сроков хранения Персональных данных Компания примет во внимание как минимум следующие аспекты:

a) Персональные данные хранятся, по крайней мере, до тех пор, пока они будут необходимы для достижения цели обработки;

b) Условия хранения Персональных данных согласуются с условиями хранения, определенными законодательством в соответствии с целью хранения Персональных данных;

c) Персональные данные хранятся до тех пор, пока Компания должна хранить доказательства в случае возбуждения судебного иска и / или спора;

d) Персональные данные не могут быть удалены из документов, если такое удаление оказывает влияние на юридическую силу документа.

## 13. СРОК ХРАНЕНИЯ ДАННЫХ

13.1. Персональные данные, обрабатываемые в рамках деятельности Контролера, будут храниться на протяжении всего периода, установленного договором (трудоустройство работника, оказание услуги/ закупки материалов и т. д. Контролером), а также в течение срока, необходимого для достижения целей, для которых они были собраны, или для защиты законных интересов Контролера, связанных с ним подразделений и/или его сотрудников и партнеров.

13.2. По истечении юридического / договорного срока хранения Персональные данные и / или документы на электронном или бумажном носителе уничтожаются, анонимизируются или, при определенных обстоятельствах, передаются в государственные архивы. Каждое лицо, ответственное за процесс обработки Персональных данных, несет ответственность за выполнение удаления или процесс анонимизации.

13.3. При прекращении отношений, лежащих в основе обработки данных Субъектов данных Контролером, носители персональных данных передаются в архив Контролера и хранятся в течение следующих установленных сроков хранения:

- персональные данные о партнерах и подрядчиках или полученные от них: через 5 лет после завершения установленных отношений;

- персональные данные в отношении работников: 75 лет с момента прекращения действия индивидуальных трудовых договоров.

13.4. Срок хранения может отличаться от указанного, если в указателе типовых документов и сроков их хранения для организаций и предприятий РМ указан другой срок хранения. В таком случае данные будут храниться в течение периода, установленного в указателе типовых документов. В случае возникновения спора данные будут обрабатываться в течение срока,

необходимого для защиты законных интересов Контролера и связанных с ним лиц.

## 14. УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

14.1. Информация, которая содержит персональные данные и больше не требуется для достижения целей обработки, определенных Компанией, и хранение которых не предусмотрено применимым законодательством, должна быть уничтожена. Электронная информация уничтожается таким образом, чтобы восстановление файлов было невозможно. Данные в письменной форме (на бумажном носителе) уничтожаются таким образом, чтобы восстановление содержащихся сведений было невозможно.

14.2. Запрещается передавать (отчуждать) информационные устройства третьим лицам в случае, если они содержат Персональные данные. Вышеупомянутый запрет также должен соблюдаться в тех случаях, когда ИТ-устройства передаются для использования. Если ИТ-устройство нуждается в ремонте в рамках гарантийных обязательств, перед отправкой на ремонт необходимо обеспечить безопасность содержащихся на нем Персональных данных.

14.3. Персональные данные, которые стали неполными, устаревшими, фальсифицированными, незаконно обработанными или больше не нужны для достижения целей обработки Персональных данных, определенных Компанией, немедленно исправляются, обновляются или удаляются.

14.4. По завершении процесса обработки Персональных данных и/или по истечении срока их хранения, если Персональные данные не являются анонимными, Компания или Уполномоченное лицо удалит личные данные из информационной системы таким образом, чтобы их восстановление было невозможным.

14.5. Бумажные документы, содержащие Персональные данные или их черновики, уничтожаются в установленном законодательством порядке после обработки данных и/или истечения срока хранения, если они не переданы в архив.

14.6. После окончания необходимости их использования технические ресурсы, содержащие персональные данные (USB, CD, HDD и т.д.), передаются в отдел информационных технологий компании, который централизованно уничтожает технические ресурсы, чтобы невозможно было восстановить сохраненную информацию и удалить ее.

14.7. Удаление Персональных данных регистрируется (документируется) путем подготовки акта об уничтожении Персональных данных в случае необходимости, при этом не допускается включения в соответствующий акт информации о том, какие именно Персональные данные были уничтожены.

## 15. УПРАВЛЕНИЕ И РЕГИСТРАЦИЯ ИНЦИДЕНТОВ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

15.1. Лицо, вовлеченное в обработку Персональных данных, обнаружившее угрозу, должно немедленно уведомить ответственное лицо и специалиста по защите данных Компании о любой угрозе, связанной с обработкой Персональных данных, в том числе описанные ниже, используя номер телефона, установленный Компанией для этой цели и / или адрес электронной почты:

- если обнаружена угроза техническим ресурсам, включая ИТ-ресурсы (например, отключение электропитания, наличие жидкостей или частиц, повреждение от физического воздействия, пожар или наводнение, потеря или кража компьютеров и других технических средств и т.д.);

- если обнаружена угроза Информационным ресурсам (например, Третьи лица узнали пароль, обнаружен несанкционированный доступ к Персональным данным, включая потерю USB-носителей информации, компакт-дисков, а также отправку электронного письма, содержащего Персональные данные, непредусмотренным адресатам, перебои в работе Информационной системы, несанкционированное удаление или исправление Персональных данных;

- если обнаружен какой-либо вид угрозы Персональным данным в бумажном формате (например, слишком высокая влажность в помещении, неисправность замка на шкафу или дверях в помещении, неработающая сигнализация, доступ третьих лиц к документам, потеря документов и т.д.).

15.2. В случае угрозы лицо, участвующее в обработке Персональных данных, должно обеспечить безопасность компьютерной системы в пределах своих полномочий и авторизации до прибытия Ответственного лица.

15.3. При поступлении уведомления о возникновении инцидента в области безопасности лицо, ответственное за расследование инцидента в области безопасности, выполняет следующие действия:

- оценивает, какие лица в Компании должны быть уведомлены о возможном Инциденте в области безопасности, с тем чтобы немедленно ограничить воздействие Инцидента в области безопасности, минимизировать последствия, купировать действие и последствия Инцидента в области безопасности, предотвратить повторение Инцидента в области безопасности;

- оценивает меры, которые необходимо осуществить для прекращения Инцидента в области безопасности (если он не завершился), ограничения негативного воздействия Инцидента в области безопасности на Заинтересованное лицо (Субъекта данных), минимизации любых потерь, и немедленно начинает их реализацию;

- оценивает, нужно ли уведомлять об Инциденте в области безопасности полиции (если он имеет признаки преступления) или уполномоченным законом властям;

- оценивает риск, связанный с Инцидентом в области безопасности и частной жизнью физических лиц, посредством оценки следующих аспектов:

  a) Были ли затронуты инцидентом в сфере безопасности Персональные данные?
  b) Какие именно Персональные данные были затронуты?
  c) Насколько конфиденциальны данные, затронутые в результате инцидента в сфере безопасности, являются ли они данными особой категории?
  d) Какие лица могут быть затронуты/на какие лица может быть оказано негативное воздействие в результате инцидента в сфере безопасности, включая количество и категории пострадавших?
  e) Как и почему произошел Инцидент в сфере безопасности?
  f) Если данные были утеряны или похищены, может ли Третья сторона узнать что-либо о соответствующем лице на основании данных, которые были утеряны или похищены?
  g) Каким будет воздействие/последствия инцидента безопасности для вовлеченных лиц, включая возможную угрозу физической безопасности этих лиц, нанесение имущественного, репутационного или морального ущерба?
  h) Если данные были утеряны или похищены, были ли данные анонимизированы, закодированы, защищены паролем или каким-либо иным образом?
  i) Если данные были утеряны или похищены, могут ли они быть использованы в преступных целях?

j) Каково будет влияние/последствия Инцидентов в сфере безопасности для Компании, в том числе, могут ли они угрожать безопасности Компании и/или Заинтересованных лиц / Субъектов данных (санкции со стороны органов государственного управления, требования со стороны Заинтересованного лица / Субъекта данных), репутационный ущерб)?

k) Каковы личные данные и контакты Заинтересованных лиц / Субъектов данных, пострадавших от Инцидента в сфере безопасности, чтобы с ними можно было связаться в случае необходимости?

15.4. Контролер персональных данных письменно информирует Национальный Центр защиты Персональных данных об обнаруженных Инцидентах в сфере безопасности.

15.5. Уведомление об Инциденте в сфере безопасности, направленное в Надзорный орган, должно содержать следующую информацию:

- сведения об инциденте в сфере безопасности краткое описание инцидента в сфере безопасности;
- категории Заинтересованных лиц / Субъектов данных, вовлеченных в Инцидент в сфере безопасности, приблизительное количество пострадавших Заинтересованных лиц / Субъектов данных (область применения затронутых Персональных данных);
- фамилия, имя и контактные данные специалиста в области защиты данных или ссылка на контактные данные другого лица, от которого Заинтересованное лицо / Субъект данных может получить дополнительную информацию;
- Последствия инцидента в сфере безопасности или возможные последствия инцидента в области безопасности;
- Меры, принятые или запланированные Компанией в целях смягчения возможных негативных последствий Инцидента в сфере безопасности и для предотвращения возникновения таких Инцидентов в сфере безопасности в будущем;
- Другие сведения, если это предусмотрено действующим законодательством, в случае специального уведомления, а также иная информация, рассматриваемая Компанией как необходимая.
- Лицо, ответственное за регистрацию Инцидентов в сфере безопасности, должно оценить каждое полученное уведомление, относящееся к Инциденту в сфере безопасности, и, если инцидент следует рассматривать как нарушение защиты Персональных данных и как обстоятельство, могущее вызвать высокий риск для прав и свобод физических лиц, Ответственное лицо должно

уведомить Субъекта данных, затронутого в результате Инциденте в сфере безопасности, об Инциденте безопасности.

## 16. ВИДЕОНАБЛЮДЕНИЕ

16.1. Контролер использует систему видеонаблюдения в пределах допустимых параметров.

16.2. Конфиденциальность: само собой разумеется и признано, что существует законное ожидание определенной степени конфиденциальности сотрудников на рабочем месте, но это право должно быть сбалансировано с законными правами и интересами Контролера, в особенности с правом эффективно управлять своей деятельностью и правом защищать себя от ответственности перед третьими лицами, которую могут на него навлечь члены коллектива.

## 17. МАРКИРОВКА ДОКУМЕНТОВ

17.1. Вся информация, которая подлежит раскрытию и содержит персональные данные, должна быть отмечена путем включения регистрационного номера в Регистр учета Контролеров персональных данных в соответствии с Приложением 2.

## 18. ОТВЕТСТВЕННОСТЬ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ ИНФОРМАЦИИ С ОГРАНИЧЕННОЙ ДОСТУПНОСТЬЮ

18.1. Контролер персональных данных, лицо, уполномоченное контролером, третьи лица, в зависимости от обстоятельств, подписавшие приложение № 1, за несоблюдение положений политики безопасности – несет гражданскую (Гражданский кодекс), административную (ст. $74^1$ Административного кодекса) и уголовную (ст. 177, 178, 180 Уголовного кодекса) ответственность.

## 19. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

19.1. Настоящая Политика безопасности дополняется положениями действующего законодательства.

19.2. Изменение и заполнение настоящей Политики безопасности осуществляется в порядке, установленном для ее утверждения.

19.3. Содержание Политики безопасности ежегодно пересматривается и обновляется, чтобы отразить любые изменения в требованиях к

предпринимательской деятельности Контролера, ИТ-рисках или значительных угрозах Информационным Системам.

Приложение 1

к Политике безопасности в сфере
обработки Персональных данных в рамках
деятельности SRL " NEW POST
INTERNATIONAL"

**КАТЕГОРИИ**
**персональных данных**

1. Персональные данные, которые прямо или косвенно идентифицируют физическое лицо, в частности, со ссылкой на идентификационный номер (персональный код), на один или несколько специфических элементов, свойственных его физической, физиологической, психической, экономической, культурной или социальной идентичности, делятся на две категории: обычные и специальные.

2. К категории обычных относятся данные, которые раскрывают:
   1) фамилию и имя;
   2) пол;
   3) дату и место рождения;
   4) гражданство;
   5) персональный идентификационный код IDNP
   6) фотоизображение;
   8) семейное положение;
   9) статус военнообязянного;
   10) персональные данные членов семьи;
   11) данные, указанные в водительском удостоверении;
   12) данные из свидетельства о регистрации;
   13) экономическое и финансовое положение;
   14) данные о владении имуществом;
   15) банковские реквизиты;
   17) подпись;
   18) данные актов гражданского состояния;
   19) номер пенсионного досье;
   20) персональный код социального страхования (CPAS);
   21) персональный код медицинского страхования (CPAM);
   22) номер телефона / факса;
   23) номер мобильного телефона
   24) адрес (проживания / пребывания);
   25) адрес электронной почты;

27) профессия и / или место работы;
28) профессиональная подготовка – дипломы – сведения об образовании;

3. Особые категории персональных данных – данные, раскрывающие расовое или этническое происхождение лица, политические убеждения, религиозные или философские воззрения, социальную принадлежность, данные, касающиеся состояния здоровья или половой жизни, а также данные, касающиеся уголовного наказания, принудительных процессуальных мер или санкций за правонарушения; Контролер не обрабатывает особые категории персональных данных.

Приложение 2

к Политике безопасности в сфере обработки Персональных данных в рамках деятельности SRL " NEW POST INTERNATIONAL"

1. **Образец предупреждающего знака:**

   Внимание! Документ содержит персональные данные, обрабатываемые в рамках системы записи № _____, зарегистрированной в Регистре контролеров персональных данных www.registru.datepersonale.md. Последующая обработка этих данных может осуществляться только в соответствии с условиями, предусмотренными Законом № 133 от 08.07.2011 о защите персональных данных.

2. **Пример маркировки видеонаблюдения:**

   В соответствии с авторизацией Национального центра защиты персональных данных Республики Молдова, New Post International S.R.L. контролирует зону видео:

   Обращение с жалобой на обработку персональных данных посредством данной системы учета в адрес Национального центра защиты персональных данных Республики Молдова может быть осуществлено только после предварительной подачи заявления контролеру персональных данных.

Пример: **Форма согласия на трансграничную передачу персональных данных:**

В соответствии с положениями Закона 133 от 08.07.2011 о защите персональных данных NEW POST INTERNATIONAL MLD SRL со штаб-квартирой в мун. Кишинэу, бул. Штефан чел Маре 65, оф. 806, государственный идентификационный номер - налоговый код 1014600029674 («**Компания**» «**Контролер**») производит сбор и обработку некоторых относящихся к вам персональных данных. Эти данные представляют собой любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу.

Собранные данные подлежат трансграничной передаче, хранятся на серверах Оператора, расположенных в Украине, обрабатываются компанией New Post S.R.L., зарегистрированной в соответствии с законодательством Украины, регистрационный номер 31316718, юридическое местонахождение которой находится в Украине, г. Киев, шоссе Столичное 103, блок 1, 9 эт., в качестве импортера данных. Импортер данных обрабатывает данные в объеме и в условиях, установленных соглашением о передаче персональных данных, подписанным Контролером и импортером данных.

В целях соответствия действующему законодательству и в целях сотрудничества между Компанией и субъектом персональных данных («**Субъект**»), Субъект на основании настоящего выражает свое свободное, безусловное, явное и сознательное согласие и подтверждает следующее:

1. Настоящим субъект персональных данных соглашается с трансграничной передачей Компанией своих персональных данных, данных, включающих все или некоторые из следующих категорий: имя, фамилию и отчество; пол, подпись, электронную подпись, персональный государственный идентификационный номер (IDNP); дату и место рождения; гражданство, данные актов гражданского состояния, код личного медицинского страхования (CPAM) мобильный телефон, домашний адрес/место жительства телефон/ факс, электронную почту, профессию, должность, профессиональную подготовку - дипломы - сведения об образовании, семейное положение, данные членов семьи экономическое или финансовое положение, размер зарплаты брутто, премии, надбавки, поощрения, сведения из больничных листов, банковские реквизиты, фотографии, данные из водительского удостоверения, сведения о дисциплинарных взысканиях, персональный код социального страхования (CPAS), персональный код медицинского страхования, данные из свидетельства о регистрации, место работы, прочие: больничный лист, размер заработной платы брутто, премии, поощрения, дополнительные выплаты.

2. Субъект персональных данных настоящим принимает и соглашается с тем, что его персональные данные будут передаваться Компанией трансгранично для следующих целей:

a) Выполнение договоров между Субъектом и компанией;

b) Другие ситуации, связанные с договорными отношениями, которые Субъект данных имеет или будет иметь с Компанией.

3. Субъект персональных данных соглашается и принимает, что его персональные данные могут быть переданы New Post S.R.L. в соответствии с законом.

4. Субъект персональных данных настоящим соглашается и принимает, что данное согласие действует в течение пяти лет и может быть продлено на последующие пятилетние периоды. Согласие на обработку персональных данных может быть отозвано в любое время до истечения срока, посредством письменного, датированного и подписанного заявления, поданного в офис Контролера.

5. Субъект персональных данных подтверждает знание положений Закона о защите персональных данных (№133 от 8 июля 2011 г.) , признавая, что в связи с обработкой данных Компанией она имеет следующие права, как это установлено законом:

- Право на получение информации о личности контролера или обработчика, цели обработки собранных данных, а также дополнительной информации о получателях персональных данных;
- Право доступа к своим персональным данным;
- Право на вмешательство в персональные данные;
- Право на возражение;
- Право не оказаться под воздействием частного решения;
- Право на доступ к правосудию.

Для осуществления этих прав субъект персональных данных вправе подать письменное, датированное и подписанное заявление в офис Контролера.

6. Субъект персональных данных, в соответствии со ст. 17 Закона об электронной коммерции (№ 284 от 22 июля 2004 г.), соглашается на обработку своих персональных данных и выражает согласие на получение коммерческой информации в электронном виде.

**СОГЛАСИЕ**

Я заявляю, что был полностью проинформирован об обработке персональных данных Компанией и полностью прочитал, согласен и принимаю все пункты Формы согласия, касающиеся трансграничной передачи персональных данных. До моего сведения были доведены документы Компании по защите персональных данных, включая Приказ Компании о защите персональных данных. Я понимаю, что Компания может получать, собирать, объединять, организовывать, использовать, хранить, обрабатывать, передавать и раскрывать персональные данные о моей личности, как указано в настоящей Форме согласия. Я заявляю, что понимаю и согласен с тем, что персональные данные могут быть собраны, обработаны, использованы, переданы или раскрыты, и что Компания оставляет за собой право осуществлять эти действия, когда считает это необходимым, и что персональные данные могут быть переданы другим организациям как внутри, так и за пределами Республики Молдова, как указано выше в настоящей Форме согласия.

**Ф.И.О.: _____**

**Дата** **Подпись**