СОГЛАШЕНИЕ ОБ ОБРАБОТКЕ ДАННЫХ

Настоящее Соглашение об обработке данных (далее – «Соглашение») заключено между компанией Siemens Product Lifecycle Management Software Inc., также называемой Siemens Industry Software (далее – «SISW») и клиентом, подтвердившим своей подписью согласие с условиями настоящего Соглашения (далее – «Клиент»). SISW оставляет за собой право привлекать дочерние компании для реализации своих прав и исполнения своих обязательств по настоящему Соглашению. Таким образом, термин «SISW», используемый в данном документе, также обозначает дочерние компании, владение или управление которыми прямым или косвенным образом осуществляет головная материнская компания Siemens Product Lifecycle Management Software Inc. и компания, уполномоченная компанией Siemens Product Lifecycle Management Software Inc. предоставлять облачные услуги SISW (далее – «Облачные услуги»).

Клиент несет исключительную ответственность за определение типа данных и лиц, на которых влияет обработка, и должен убедиться в законности такой обработки через Облачные услуги. Клиент также должен нести ответственность за все исправления, удаление или блокирование персональных данных с помощью функционала, предоставляемого Облачными услугами. Клиент может экспортировать и удалять данные, включая персональные данные, используя функционал, предоставляемый Облачными услугами. После расторжения настоящего Соглашения об обработке данных Клиент в течение 30 дней должен направить в SISW письменный запрос на предоставление доступа к данным Клиента для загрузки. По истечении периода времени, указанного компанией SISW по такому запросу, все оставшиеся данные Клиента могут быть удалены без возможности восстановления доступа Клиента к этим данным. SISW и Клиент пришли к соглашению, что в пределах Облачной структуры право Клиента на издание инструкций будет реализоваться исключительно с помощью функционала Облачных услуг. Для дополнительных инструкций, касающихся данных Клиента, необходимо заключить отдельное письменное соглашение между SISW и Клиентом, включая соглашение о дополнительных платежах, которые должен совершить Клиент для изготовления таких инструкций. Клиент обязуется не выгружать и не хранить в хранилищах Облачных услуг охраняемой информации о здоровье (PHI), если между SISW и Клиентом не заключено отдельное письменное соглашение, в котором содержится явное разрешение на хранение PHI в хранилищах Облачных услуг.

При предоставлении Облачной услуги в рамках продуктивной системы SISW должна обеспечить выполнение технических и организационных мер, описанных в Дополнении 2 к Приложению А настоящего Соглашения об обработке данных. В отношении тестовых систем, относящихся к Облачной службе, могут соблюдаться или не соблюдаться меры, описанные в Дополнении 2 к Приложению А. Кроме того, SISW может периодически вносить изменения в технические и организационные меры, применимые к продуктивной системе, если эти изменения не оказывают негативного влияния на уровень защиты, обеспечиваемый такими мерами в любом вещественном выражении. SISW должна запретить сотрудникам компании сбор, обработку или использование персональных данных без соответствующего разрешения и будет возлагать обязанности, связанные с обработкой персональных данных Клиента, только на сотрудников, получивших специальные инструкции в соответствии с требованиями к обеспечению секретности данных.

SISW должна иметь право привлекать субподрядчиков в ходе оказания Облачных услуг. В тех случаях, когда доступ субподрядчика к персональным данным Клиента неизбежен, SISW по запросу Клиента будет предоставлять список таких субподрядчиков и данных об их расположении, а также она будет обновлять этот список перед тем, как доступ к персональным данным Клиента будет предоставлен новому субподрядчику. Если Клиент обоснованно возражает против нового субподрядчика, Клиент должен проинформировать SISW об этом возражении и, если SISW настаивает на добавлении нового субподрядчика, должен иметь право расторгнуть настоящее Соглашение об обработке данных по убедительной причине. В случаях, когда привлечение такого субподрядчика влечет за собой передачу персональных данных через государственную границу, SISW примет меры по обеспечению адекватного уровня защиты таких персональных данных.

SISW будет регулярно проверять соблюдение применимых технических и организационных мер и – по обоснованному запросу Клиента – предоставлять Клиенту подтверждение соблюдения применимых технических и организационных мер. Если у Клиента есть основания предполагать, что подтверждение, предоставленное компанией SISW, некорректно, Клиент должен иметь право получить подтверждение соблюдения технических и организационных мер, запланировав аудиторскую проверку с компанией SISW при условии предварительного извещения в разумный срок. Такая аудиторская проверка должна выполняться за счет Клиента.

SISW и Клиент пришли к соглашению о том, что любая передача персональных данных Клиента из стран Европейского Союза в страны, не входящие в ЕС и признанные ЕС обеспечивающими недостаточный уровень

защиты персональных данных, будет выполняться в соответствии со стандартными положениями договоров в ЕС, которые изложены в Приложении А и полностью соблюдены в настоящем Соглашении. В случае обнаружения несоответствия между условиями настоящего Соглашения об обработке данных и стандартными положениями договоров следует руководствоваться стандартными положениями договоров. Стандартные положения договоров определяются законами государства, входящего в ЕС, в котором находится экспортер данных (как указано в Приложении А).

Приложение A
Стандартные положения договоров в ЕС

Во исполнение Статьи 26(2) Директивы 95/46/ЕС о передаче персональных данных обработчикам, расположенным в третьих странах, в которых не обеспечивается достаточный уровень защиты данных

между

Клиентом и/или дочерней компанией Клиента, расположенной в ЕС

(далее – «**экспортер данных**»),

и

компанией Siemens Product Lifecycle Management Software Inc., также называемой Siemens Industry Software, включая все дочерние компании, владение или управление которыми прямо или косвенно осуществляет головная материнская компания Siemens Product Lifecycle Management Software Inc. и компания, уполномоченная компанией Siemens Product Lifecycle Management Software Inc. выполнять обработку данных по ее поручению

(далее – «**импортер данных**»),

далее называемые «сторона» или «стороны»,

ЗАКЛЮЧИЛИ СОГЛАШЕНИЕ о соблюдении описанных далее договорных положений (далее – «Положения») с целью принятия достаточных мер для защиты частной жизни и основных прав и свобод человека при передаче персональных данных, указанных в Дополнении 1, от экспортера данных к импортеру данных.

Раздел 1. Определения

Во исполнение Положений:

(a) понятия «персональные данные», «специальные категории данных», «обработка», «контролер», «обработчик», «субъект данных» и «контролирующая организация» следует трактовать в соответствии с определениями Директивы 95/46/ЕС Европейского парламента и Совета ЕС от 24 октября 1995 года о защите частных лиц при обработке персональных данных и свободном перемещении таких данных;

(b) «экспортер данных» – контролер, осуществляющий передачу персональных данных;

(c) «импортер данных» – обработчик, подтверждающий прием от экспортера данных персональных данных, которые необходимо обработать по его поручению после того, как данные будут переданы в соответствии с инструкциями экспортера и условиями Положений; на такого обработчика не должны распространяться законы третьей страны, что обеспечит достаточный уровень защиты в рамках требований статьи 25(1) Директивы 95/46/ЕС;

(d) «субподрядчик» – любой обработчик, привлекаемый импортером данных или любым другим субподрядчиком импортера данных, подтвердивший получение от импортера данных или от любого другого субподрядчика импортера данных персональных данных, предназначенных исключительно для обработки по поручению экспортера данных после того, как они будут переданы в соответствии с его инструкциями, условиями Положений и условиями письменного субдоговора;

(e) «применяемый закон о защите данных» – закон, защищающий основные права и свободы человека и в особенности их право на частную жизнь в отношении обработки персональных данных, применяемый к контролеру данных в государстве-участнике, в котором находится экспортер данных;

(f) «технические и организационные меры по обеспечению безопасности» – меры по защите персональных данных от случайного или незаконного уничтожения или случайной утери, изменения, несанкционированного раскрытия или доступа, особенно когда при обработке происходит передача данных по сети, и от всех остальных незаконных форм обработки.

Раздел 2. Сведения о передаче

Сведения о передаче и в особенности специальные категории персональных данных (если используются) указаны в Дополнении 1, которое является составной частью Приложения А.

Раздел 3. Положение о стороннем бенефициаре

1. Субъект данных как сторонний бенефициар может требовать от экспортера данных соблюдения настоящей статьи, пунктов 4(b) – (i), пунктов 5(a) – (e) и (g) – (j), пунктов 6.1 и 6.2, статьи 7, пункта 8.2, а также статей 9 – 12.

2. Субъект данных может требовать от импортера данных соблюдения этого настоящей статьи, пунктов 5(a) – (e) и (g), статьи 6, статьи 7, пункта 8.2, а также статей 9 – 12 в случаях, когда экспортер данных фактически пропал или перестал существовать по закону кроме случаев, когда организация-правопреемник взяла на себя все законные обязательства экспортера данных по договору или по закону, в результате чего она приняла права и обязанности экспортера данных, и субъект данных может потребовать их исполнения от такой организации.

3. Субъект данных может требовать от субподрядчика соблюдения этого настоящей статьи, пунктов 5(a) – (e) и (g), статьи 6, статьи 7, пункта 8.2, а также статей 9 – 12 в случаях, когда экспортер и импортер данных фактически пропали, перестали существовать по закону или стали неплатежеспособными кроме случаев, когда организация-правопреемник взяла на себя все законные обязательства экспортера данных по договору или по закону, в результате чего она приняла права и обязанности экспортера данных, и субъект данных может потребовать их исполнения от такой организации. Такая ответственность сторонней организации относительно субподрядчика должна быть ограничена собственными операциями по обработке согласно Положениям.

4. Стороны не возражают против субъекта данных, которого представляет объединение или другой орган, если субъект данных явно выражает такое желание и если это разрешено национальным законом.

Раздел 4. Обязанности экспортера данных

Экспортер данных принимает следующие условия и гарантирует их исполнение:

(a) обработка персональных данных, включая сам процесс передачи, выполняется и будет выполняться согласно соответствующим положениям применимого закона о защите данных (и, если требуется, о ней уведомлены соответствующие органы государства-участника, в котором находится экспортер данных) и не нарушает соответствующие стандартные положения договоров этого государства;

(b) экспортер проинструктирован сам и на протяжении периода оказания услуг по обработке персональных данных будет инструктировать импортера данных об обработке переданных персональных данных только по поручению экспортера данных и в соответствии с применимым законом о защите данных и Положениями;

(c) импортер данных предоставит достаточные гарантии принятия технических и организационных мер обеспечения безопасности, указанных в Дополнении 2 к Приложению А к настоящему Соглашению;

(d) после оценки требований применимого закона о защите данных будут приняты меры обеспечения безопасности, достаточные для защиты персональных данных от случайного или незаконного уничтожения или случайной утери, изменения, несанкционированного раскрытия или доступа особенно в случаях, когда обработка предусматривает передачу данных по сети, и от всех остальных незаконных форм обработки, а также эти меры обеспечивают уровень защиты, соответствующий рискам, возникающим при обработке, и природе данных, которые следует защитить, в соответствии с современным уровнем развития техники и стоимостью их реализации;

(e) экспортер будет проверять соблюдение мер обеспечения безопасности;

(f) если следует передать специальные категории данных, субъект данных проинформирован или будет проинформирован заранее или как можно раньше после передачи о том, что его данные могут быть переданы в третью страну, в которой не обеспечивается достаточный уровень защиты в соответствии с Директивой 95/46/ЕС;

(g) любые уведомления, полученные от импортера данных или любого субподрядчика в соответствии с пунктом 5(b) и пунктом 8.3, будут перенаправлены контролирующей организации, занимающейся вопросами защиты данных, если экспортер данных решит продолжить передачу данных или отменить решение о приостановке;

(h) субъекты данных по запросу могут получить копию Положений, кроме Дополнения 2, и краткое описание мер безопасности, а также копию всех договоров о субподрядных услугах, которые должны быть заключены в соответствии с Положениями кроме случаев, когда Положения или договор включают коммерческую информацию – такая коммерческая информация может быть удалена;

(i) в случае привлечения субподрядчика обработка данных осуществляется в соответствии со статьей 11, при этом субподрядчик должен обеспечить уровень защиты персональных данных и прав субъекта данных не ниже, чем у импортера данных согласно Положениям;

(j) экспортер гарантирует соблюдение пунктов 4(a) – (i).

Раздел 5. Обязанности импортера данных

Импортер данных принимает следующие условия и гарантирует их исполнение:

(a) выполнение обработки персональных данных только по поручению экспортера данных и в соответствии с его инструкциями и Положениями; если по каким-либо причинам соответствие этим требованиям невозможно, импортер соглашается немедленно проинформировать экспортера данных о невозможности соблюсти требования, в этом случае экспортер данных может временно приостановить передачу данных и/или расторгнуть договор;

(b) у импортера нет оснований полагать, что применимые к нему законы не позволяют ему выполнять требования, полученные от экспортера данных, и его обязанности по договору, а также в случае изменения этих законов, если это может оказать значительное негативное влияние на гарантии и обязанности, указанные в Положениях, импортер при получении такой информации немедленно

уведомит экспортера данных об изменениях, в этом случае экспортер данных имеет право приостановить передачу данных и/или расторгнуть договор;

(c) импортер принял технические и организационные меры обеспечения безопасности, указанные в Дополнении 2, перед выполнением обработки переданных ему персональных данных;

(d) импортер немедленно уведомит экспортера данных о следующем:

(i) любой юридически обязательный запрос органов правопорядка на раскрытие персональных данных, за исключением иных запрещенных законом случаев, например, запрет уголовного кодекса на защиту конфиденциальных данных в период проведения следственных мероприятий органами правопорядка,
(ii) любой случайный или несанкционированный доступ и
(iii) любой запрос, полученный непосредственно от субъектов данных, на который не следует отвечать, если импортер не уполномочен делать это;

(e) импортер должен быстро и надлежащим образом обрабатывать все запросы экспортера данных, связанные с обработкой передаваемых персональных данных, и следовать рекомендациям контролирующей организации относительно обработки переданных данных;

(f) импортер данных по запросу экспортера данных должен предоставить свое оборудование для обработки данных для проведения аудиторской проверки операций обработки, определенных в Положениях, которую должен провести экспортер данных или инспекционный орган, состоящий из независимых участников, имеющих необходимую профессиональную квалификацию и взявших на себя обязательства по соблюдению конфиденциальности, выбранный экспортером данных по соглашению (если применяется) с контролирующей организацией;

(g) импортер данных должен предоставить субъекту данных по его запросу копию Положений или существующего договора о субподряде кроме случаев, когда Положения или договор содержат коммерческую информацию, в этом случае импортер может удалить эту коммерческую информацию, исключая Дополнение 2, которое следует заменить кратким описанием мер обеспечения безопасности в случаях, когда субъект данных не может получить копию документов от экспортера данных;

(h) в случае заключения договора субподряда импортер данных заранее информирует экспортера данных и получает предварительное письменное согласие;

(i) субподрядчик оказывает услуги по обработке данных в соответствии со статьей 11;

(j) импортер данных немедленно отправляет экспортеру данных копию каждого соглашения с субподрядчиком, заключенного согласно Положениям.

Раздел 6. Ответственность

1. Стороны согласны с тем, что любой субъект данных, понесший ущерб в результате любого нарушения обязательств, описанных в Положении 3 или в Положении 11, любой из сторон или субподрядчиком, имеет право получить компенсацию за понесенный ущерб от экспортера данных.

2. Если субъект данных не может подать иск на получение от экспортера данных компенсации ущерба в соответствии с параграфом 1, возникшего в результате невыполнения импортером данных или его субподрядчиком обязанностей, закрепленных в Положении 3 или в Положении 11, поскольку экспортер

данных фактически пропал, перестал существовать по закону или стал неплатежеспособным, импортер данных согласен с тем, что субъект данных может подать иск в отношении импортера данных как экспортера данных кроме случаев, когда организация-правопреемник взяла на себя все законные обязательства экспортера данных по договору или по закону, в результате чего субъект данных может потребовать соблюдения его прав от этой организации.

Импортер данных не может надеяться на невыполнение обязанностей со стороны субподрядчика во избежание исполнения собственных финансовых обязательств.

3. Если субъект данных не может подать иск на получение от экспортера данных или импортера данных компенсации ущерба в соответствии с параграфом 1 и 2, возникшего в результате невыполнения субподрядчиком обязанностей, закрепленных в Положении 3 или в Положении 11, поскольку экспортер данных и импортер данных фактически пропали, перестали существовать по закону или стали неплатежеспособными, субподрядчик согласен с тем, что субъект данных может подать иск в отношении субподрядчика в рамках его собственных операций обработки, закрепленных в Положениях, как в отношении экспортера или импортера данных кроме случаев, когда организация-правопреемник взяла на себя все законные обязательства экспортера или импортера данных по договору или по закону, в результате чего субъект данных может потребовать соблюдения его прав от этой организации. Финансовая ответственность субподрядчика должна быть ограничена собственными операциями по обработке согласно Положениям.

Раздел 7. Посредничество и юрисдикция

1. Импортер данных соглашается с тем, что если субъект данных ходатайствует против прав стороннего бенефициара и/или подает иск о компенсации ущерба согласно Положениям, импортер данных согласится с решением субъекта данных:

   (a) при возникновении разногласий привлекать независимое лицо или (если доступно) контролирующую организацию для содействия в примирении сторон;

   (b) при возникновении разногласий обращаться в суд в государстве-участнике, в котором находится экспортер данных.

2. Стороны согласны с тем, что выбор, сделанный субъектом данных, не нанесет ущерба их материальным или процессуальным правам, связанным с выбором средств защиты права в соответствии с другими положениями национального или международного законодательства.

Раздел 8. Взаимодействие с контролирующими организациями

1. Экспортер данных согласен с тем, что копия настоящего договора будет храниться в контролирующей организации, если она ее запросила или если это предусматривает применимый закон о защите данных.

2. Стороны согласны с тем, что контролирующая организация имеет право проводить аудиторскую проверку импортера данных и любых субподрядчиков, если аудиторская проверка выполняется в том же объеме и в тех же обстоятельствах, что и аудиторская проверка экспортера данных, выполняемая согласно применимому закону о защите данных.

3. Импортер данных должен немедленно уведомить экспортера данных о наличии закона, применимого к нему или любому субподрядчику, который запрещает проведение аудиторской проверки импортера данных или

любого субподрядчика согласно пункту 2. В таком случае экспортер данных должен иметь право принять меры, предусмотренные в пункте 5 (b).

Раздел 9. Регулирующее законодательство

Положения должны соответствовать нормам законодательства государства-участника, в котором находится экспортер данных.

Раздел 10. Изменение договора

Стороны обязуются не изменять Положения. Это не запрещает Сторонам при необходимости добавлять положения о вопросах, связанных с ведением коммерческой деятельности, если они не противоречат Положениям.

Раздел 11. Субподряд

1. Импортер данных не может заключать договоры субподряда на выполнение операций, которые он выполняет по поручению экспортера данных в соответствии с Положениями, без получения предварительного письменного согласия экспортера данных. Если импортер данных передает свои обязательства, на которые распространяются Положения, субподрядчикам при наличии согласия экспортера данных, он должен заключить с субподрядчиком письменное соглашение, по которому на субподрядчика возлагаются те же обязательства, что и на импортера данных согласно Положениям. Если субподрядчик не может выполнить свои обязательства по защите данных согласно письменному соглашению, импортер данных несет полную ответственность перед экспортером данных за выполнение субподрядчиками своих обязательств согласно этому соглашению.

2. Предварительно заключенный письменный договор между импортером данных и субподрядчиком должен также включать дополнительное положение о стороннем бенефициаре, как указано в статье 3, которое применяется в случаях, когда субъект данных не может подать иск о возмещении убытков, предусмотренном пункта 1 статьи 6, в отношении экспортера данных или импортера данных, поскольку они фактически пропали, перестали существовать по закону или стали неплатежеспособными, и не возникло организации-правопреемника, которая взяла на себя все законные обязательства экспортера или импортера данных по договору или по закону. Такая ответственность сторонней организации относительно субподрядчика должна быть ограничена собственными операциями по обработке согласно Положениям.

3. Положения, связанные с вопросами защиты данных при привлечении субподрядчиков для выполнения обязательств по договору согласно пункту 1, должны регулироваться законом государства-участника, в котором находится экспортер данных.

4. Экспортер данных должен хранить список соглашений субподряда, заключенных согласно Положениям, и импортер данных должен уведомить экспортера данных согласно пункту 5 (j) о договорах, которые следует обновлять хотя бы раз в год. Список должен быть предоставлен в контролирующую организацию экспортера данных, занимающуюся вопросами защиты данных.

Раздел 12. Обязательства после прекращения оказания услуг по обработке персональных данных

1. Стороны согласны с тем, что при прекращении оказания услуг по обработке данных импортер данных и субподрядчик должны по выбору экспортера данных вернуть экспортеру данных все переданные персональные данные и их копии или уничтожить все персональные данные и подтвердить экспортеру данных их уничтожение кроме случаев, когда законы, распространяющиеся на импортера данных, запрещают возврат или уничтожение всех переданных персональных данных или их части. В этом случае

импортер данных гарантирует обеспечение конфиденциальности переданных данных и обязуется никогда не выполнять активную обработку переданных персональных данных.

2. Импортер данных и субподрядчик гарантируют, что по запросу экспортера данных и/или контролирующей организации он предоставит свое оборудование для обработки данных для проведения аудиторской проверки в отношении мер, предусмотренных в пункте 1.

ДОПОЛНЕНИЕ 1 К СТАНДАРТНЫМ ПОЛОЖЕНИЯМ ДОГОВОРА

Экспортер данных
Экспортер данных (кратко укажите операции, связанные с передачей):

Клиент является подписчиком Облачныхуслуг, оказываемых SISW, что позволяет конечным пользователям, уполномоченным Клиентом, вводить, изменять, использовать, удалять, загружать и иначе работать с данными Клиента, к которым могут относиться персональные данные согласно положениям Соглашения и относящейся к нему документации по Облачным услугам.

Импортер данных
Импортер данных (кратко укажите операции, связанные с передачей):

Компания Siemens Product Lifecycle Management Software Inc. самостоятельно или с помощью субподрядчиков оказывает Облачную услугу, которая включает следующее: поддержка вычислительной инфраструктуры в США и ЕС, через которую предоставляется Облачные услуги; сохранение в инфраструктуре данных Клиента, выгруженных Клиентом в хранилища Облачных услуг; отслеживание доступности и работы Облачных услуг и инфраструктуры; обеспечение безопасности инфраструктуры согласно условиям Соглашения и относящейся к нему документации по Облачным услугам.

Субъекты данных
Передаваемые персональные данные касаются следующих категорий субъектов данных (укажите):

Если иное явно не указано экспортером данных в письменном виде, к субъектам данных могут относиться конечные пользователи, уполномоченные Клиентом использовать Облачные услуги, и другие сотрудники Клиента, персональные данные которых хранятся в хранилищах Облачных услуг.

Категории данных
Передаваемые персональные данные касаются следующих категорий данных (укажите):

определенные категории данных, которые необходимо разместить в хранилищах Облачных услуг, должны быть тщательно сконфигурированы Клиентом, хотя существуют некоторые общие категории данных, которые могут находиться в хранилищах Облачных услуг, например (но не ограничиваясь ими): имя, адрес электронной почты, название компании, номер телефона, адрес места работы, национальность или гражданство и информация, касающаяся доступа к Облачным услугам и ее использования; в зависимости от клиентской конфигурации Облачных услуг в ее хранилищах могут быть размещены многие другие категории данных Клиента.

Специальные категории данных (если используются)
Передаваемые персональные данные касаются следующих специальных категорий данных (укажите):

в хранилище Облачных услуг можно хранить данные специальных категорий, указанных сторонами в Соглашении или в Регламенте или перечисленных в техническом задании для профессиональных услуг, которое предоставляется Клиенту при развертывании Облачных услуг.

Операции по обработке
С передаваемыми персональными данными выполняются следующие основные операции по обработке (укажите):

персональные данные могут обрабатываться: в процессе стандартной работы Облачных услуг в зависимости от конфигурации Клиента; путем хранения и/или архивации в вычислительной инфраструктуре, которые выполняет экспортер данных, в одно- или многоклиентных средах; путем доступа к ним и их передачи в соответствии с инструкциями, выпущенными для Облачной услуги конечным пользователем, уполномоченным Клиентом использовать Облачные услуги; в рамках обеспечения работы Облачных услуг экспортером данных.

ДОПОЛНЕНИЕ 2 К СТАНДАРТНЫМ ПОЛОЖЕНИЯМ ДОГОВОРА

Некоторые предложения Облачных услуг осуществляются на различных условиях, которые (если применяются) определяются в заказе. В ином случае импортер данных примет технические и организационные меры, описанные ниже, в отношении персональных данных, хранящихся в системе, в соответствии с пунктами 4(d) и 5(c) Положений.

Описание технических и организационных мер обеспечения безопасности, принимаемых импортером данных в соответствии с пунктами 4(d) и 5(c):

1. Контроль физического доступа. Следует предотвращать физический доступ неуполномоченных лиц на территорию, в здания или в помещения, в которых расположены системы обработки и/или использования персональных данных.

   Меры: все центры обработки данных соблюдают строгие меры обеспечения безопасности путем привлечения сил безопасности, использования оборудования для слежения, датчиков движения, механизмов контроля доступа и других средств предотвращения угроз для оборудования и помещений центров обработки данных. Доступ к системам и инфраструктуре в помещениях центров обработки данных имеют только уполномоченные представители. Правильность работы физического оборудования для обеспечения безопасности (например, датчики движения, камеры и т.д.) проверяется регулярно. В частности, во всех центрах обработки данных применяются следующие меры обеспечения безопасности:

   a. В целом защита зданий обеспечивается с помощью систем контроля доступа (система доступа с помощью смарт-карт).
   b. Уполномоченным сотрудникам выдаются средства доступа, включающие электронный пропуск (сотрудники, поставщики и подрядчики получают уникальные пропуски) и ПИН-код, с помощью которых они могут физически попасть в здания центров обработки данных.
   c. Физический доступ к центрам обработки данных в пределах системы обеспечивается с помощью системы контроля доступа, которая включает устройства считывания карт и клавиатуры для ввода ПИН-кода для доступа в здания и помещения, а также устройства считывания карт только для выхода из зданий и помещений.
   d. В зависимости от уровня безопасности к зданиям, отдельным пространствам и окружающей территории могут применяться дополнительные меры обеспечения безопасности. К ним относятся специальные профили доступа, системы видеонаблюдения, системы тревожной сигнализации и биометрические системы контроля доступа.
   e. Права доступа получают уполномоченные сотрудники индивидуально в соответствии с мерами по контролю систем и доступа к данным, описанными ниже. Этот принцип также применяется в отношении посетителей. Гости и посетители, приходящие в здания SISW, должны указать на стойке регистрации свое имя, их должны сопровождать уполномоченные специалисты компании SISW. SISW и сторонние поставщики решений для центров обработки данных регистрируют в центрах обработки данных имена посетителей и время их доступа в защищенные пространства SISW.
   f. Сотрудники SISW и персонал сторонних организаций должны носить карточки с идентификаторами во всех пространствах SISW.

2. Контроль доступа в систему Необходимо обеспечивать защиту систем обработки данных, используемых при предоставлении Облачных услуг, от несанкционированного использования.

   Меры:

   a. Компания SISW или ее субподрядчики управляют средой в соответствии с требованиями к контролю доступа, идентификации и аутентификации NIST SP 800-53 версии 4.
   b. Для предоставления доступа к защищенным системам, включая те из них, которые используются для хранения и обработки персональных данных, используются различные уровни авторизации. Выполняются процедуры, позволяющие гарантировать, что только авторизованные пользователи получают права на добавление, удаление или изменение данных пользователей.
   c. Любой пользователь, выполняющий доступ в системы SISW, использует уникальное имя пользователя и пароль, который должен соответствовать минимальным требованиям к его сложности.
   d. SISW и субподрядчики выполняют процедуры, гарантирующие, что запрошенные изменения в авторизации применяются только в соответствии с указаниями (например, права не предоставляются без авторизации). Если пользователь SISW изменяет роли или увольняется из компании, его права доступа к среде аннулируются.

e. SISW и субподрядчики установили политики использования паролей, согласно которым запрещается раскрытие паролей, а также в них предусмотрены действия в случае раскрытия пароля, они требуют регулярной смены всех паролей пользователей и замены паролей, заданных по умолчанию. Пользователям назначаются персональные идентификаторы для выполнения аутентификации. Все пароли должны соответствовать минимальным требованиям к их сложности и храниться в зашифрованном виде. Для паролей доменов предусмотрена автоматическая смена паролей каждые 60 дней в соответствии с минимальными требованиями к их сложности. Каждый компьютер SISW оснащен экранной заставкой, защищенной паролем.
f. SISW или ее субподрядчики выполняют автоматическую аудиторскую проверку следующих действий с учетными записями: создание, изменение, включение, отключение и удаление. Системный администратор периодически проверяет журналы данных.
g. Сети компании SISW и ее субподрядчиков защищены от публичных интернет-сетей с помощью брандмауэров.
h. Компания SISW и ее субподрядчики используют актуальное антивирусное программное обеспечение в точках доступа в сеть компании, для электронных почтовых ящиков, на всех файловых серверах и на всех рабочих станциях.
i. Компания SISW и ее субподрядчики используют средства управления исправлениями уязвимостей при развертывании соответствующих обновлений систем обеспечения безопасности.
j. Полную защиту дистанционного доступа к корпоративной сети SISW и критической инфраструктуре обеспечивает строгая многофакторная аутентификация.

3. Контроль доступа к данным. Сотрудники, имеющие право использовать системы обработки данных, получают доступ только к тем персональным данным, доступ к которым им разрешен, и чтение, копирование, изменение или удаление персональных данных невозможно без авторизации в процессах обработки, использования и хранения.

   Меры:
   a. Доступ к персональной, конфиденциальной или секретной информации предоставляется только в случае необходимости. Другими словами, сотрудники или третьи стороны получают доступ к информации, которая им необходима для выполнения своей работы. SISW использует принципы авторизации, предусматривающие документирование того, как получена авторизация и какие авторизации назначаются. Защита всех персональных, конфиденциальных или других секретных данных обеспечивается в соответствии со стандартами и политиками безопасности SISW.
   b. Управление всеми рабочими серверами любой Облачной службы SISW осуществляется в соответствующих центрах обработки данных. Проверка мер обеспечения безопасности приложений, выполняющих обработку персональных, конфиденциальных и других секретных данных, выполняется регулярно. С этой целью SISW также регулярно привлекает сторонние организации для проведения аудиторских проверок, подтверждающих правильность реализации указанных мер.
   c. SISW не разрешает установку персонального программного обеспечения или другого программного обеспечения, не утвержденного компанией SISW для использования в системах Облачных услуг.
   d. При необходимости передать данные в связи с неисправностью используемого носителя данных, после выполнения этой передачи данных, неисправный носитель данных будет размагничен (для магнитных носителей данных) или раздроблен на части (для твердотельных или оптических носителей данных).

4. Контроль передачи данных Чтение, копирование, изменение или удаление персональных данных запрещено без авторизации во время передачи.

   Меры
   a. Компания SISW или ее субподрядчики управляют инфраструктурой и конфигурацией в соответствии с требованиями по защите систем и связи NIST SP 800-53 версии 4. К средствам защиты относятся системы предотвращения вторжения по сети (NIPS) и брандмауэры на границах системы, позволяющие предотвратить возможность вредоносного подключения на внешней границе инфраструктуры. Конфигурация NIPS и брандмауэров соответствует стандартам DISA STIG. Шифрование данных выполняется в пути с помощью криптографических модулей, соответствующих стандарту FIPS 140-2.
   b. Там, где SISW выполняет физическую транспортировку носителей данных, применяются достаточные меры по обеспечению уровня безопасности, предусмотренного в соглашении (например, шифрование и освинцованные контейнеры).

c. Передача персональных данных через внутренние сети SISW защищена также, как и другие конфиденциальные данные, в соответствии с политиками обеспечения безопасности SISW.
d. При передаче данных между компанией SISW и Клиентом принимаются меры обеспечения безопасности передаваемых персональных данных, предусмотренные в Соглашении или в соответствующей документации по Облачным услугам. Этот принцип применяется как для физической, так и для сетевой передачи данных. Клиент берет на себя ответственность за любую передачу данных от Точки разграничения SISW (например, брандмауэр для исходящих соединений центра обработки данных, в котором развернуты Облачные услуги).

5. Контроль ввода данных. Облачные услуги позволяют выполнять ретроспективное определение того, кто ввел персональные данные, изменил их или удалил из инфраструктуры, используемой для предоставления Облачных услуг.

   Меры
   a. SISW разрешает доступ к персональным данным только авторизованным специалистам, если это необходимо для выполнения их работы. SISW внедрила систему регистрации операций ввода, изменения и удаления, а также блокирования персональных данных компанией SISW или ее субподрядчиками, насколько это возможно в Облачных услугах.
   b. Аудиторский след включает достаточный объем информации для реконструкции событий, если обнаружена несанкционированная деятельность или неисправная работа или если есть соответствующие подозрения. В каждом файле регистрации событий операционной системы указан тип события, временная метка, источник события, местоположение события, результат события и пользователь, связанный с событием.

6. Контроль выполнения задания. Обработка персональных данных осуществляется только в соответствии с условиями Соглашения и всеми связанными инструкциями, предоставленными Клиентом.

   Меры
   a. Компания SISW использует средства управления и процессы, обеспечивающие соблюдение договоров между SISW и ее Клиентами, субподрядчиками или другими поставщиками услуг.
   b. Для данных Клиента обеспечивается как минимум такой же уровень защиты, что и для конфиденциальной информации согласно стандарту классификации информации SISW.
   c. Все сотрудники и партнеры SISW по договору принимают на себя обязательства по соблюдению конфиденциальности всей секретной информации, включая коммерческую тайну клиентов и партнеров SISW.

7. Контроль доступности. Персональные данные защищены от случайного или несанкционированного уничтожения или утери.

   Меры:
   a. SISW выполняет процессы резервного копирования и принимает другие меры по обеспечению быстрого восстановления критических важных для компаний систем, если и когда это необходимо.
   b. SISW привлекает глобальных поставщиков облачных услуг для обеспечения центрам данных дополнительных мощностей.
   c. SISW разработала варианты плана, а также стратегии развития Облачных услуг и их восстановления после чрезвычайных ситуаций.

8. Контроль разделения данных. Обработка персональных данных, собранных для различных целей, может выполняться отдельно.

   Меры:
   a. При наличии возможности компания SISW использует технические возможности развернутого программного обеспечения (например, многоклиентные или отдельные системные среды) для разделения персональных данных Клиента и других клиентов.
   b. SISW использует отдельные экземпляры (с логическим или физическим разделением) для каждого клиента.
   c. Клиент (включая его филиалы) имеет доступ только к собственным экземплярам.

9. Контроль целостности данных, Персональные данные остаются незатронутыми, полными и актуальными при выполнении операций по обработке:

   Меры: SISW внедрила стратегию защиты на различных уровнях, которая предназначена для недопущения несанкционированных изменений. Она относится к средствам контроля, что указано в разделах о контроле и мерах выше. Настройка брандмауэров позволяет выделять сегменты сети, к которым может быть предоставлен общий или частный доступ. Каждый набор правил для брандмауэров включает специальные элементы контроля доступа, определяющие допустимые типы связи между сегментами.

   a. Центр отслеживания безопасности Программное обеспечение автоматизированного обнаружения несанкционированного доступа используется в сочетании с другим программным обеспечением для защиты и проведения экспертизы и процессом предупреждения, изучения и, если необходимо, уведомления и содействия в восстановлении нарушенной безопасности.
   b. Антивирусное программное обеспечение: во всех системах используется актуальное антивирусное программное обеспечение, настроенное для защиты от вирусов, программ-червей, троянских программ и других форм вредоносного ПО.
   c. Резервное копирование и восстановление: во всех системах предусмотрен базовый уровень моментальных снимков резервной копии данных и конфигурации. Если необходимо, компания SISW и ее субподрядчики также управляют экземпляром клиента с использованием конфигурации с высоким уровнем доступности, что гарантирует хранение данных в двух различных центрах данных на достаточном удалении друг от друга.
   d. Периодические аудиторские проверки сторонними организациями для подтверждения применения мер обеспечения безопасности. Компания SISW и ее субподрядчики подвергаются периодическим аудиторским проверкам, проводимым сторонними организациями, для тестирования мер обеспечения безопасности, перечисленных выше.