СОГЛАШЕНИЕ ОБ ОБРАБОТКЕ ДАННЫХ

Настоящее Соглашение об обработке данных ("Соглашение") является соглашением между Вами (**Клиент**) и ООО "АЙТИ ПРОВАЙД", зарегистрированной в Российской Федерации, юридический адрес которой: 350051, Краснодарский край, Краснодар г., Им. Дзержинского ул., дом 49, помещение 28 (**Поставщик**), отражающим договоренность сторон о предоставлении Поставщиком услуг по обработке данных (с периодическими изменениями) и обработке Персональных данных субъектов Клиента в соответствии с требованиями законодательства о защите данных.

Если вы принимаете настоящее Соглашение об обработке данных от имени Клиента, вы гарантируете, что: (a) вы имеете полное юридическое право связывать Клиента настоящим Соглашением об обработке данных; (b) вы прочитали и поняли настоящее Соглашение об обработке данных; и (c) вы соглашаетесь от имени Клиента с настоящим Соглашением об обработке данных. Если у вас нет законных полномочий связывать Клиента, пожалуйста, не принимайте настоящее Соглашение об обработке данных.

НАЖАВ КНОПКУ "ПРИНИМАЮ" НИЖЕ, ВЫ (А) ПОДТВЕРЖДАЕТЕ, ЧТО ПРОЧИТАЛИ И ПОНЯЛИ НАСТОЯЩЕЕ СОГЛАШЕНИЕ; (Б) ЗАЯВЛЯЕТЕ И ГАРАНТИРУЕТЕ, ЧТО У ВАС ЕСТЬ ПРАВО, ПОЛНОМОЧИЯ И ВЛАСТЬ ДЛЯ ЗАКЛЮЧЕНИЯ НАСТОЯЩЕГО СОГЛАШЕНИЯ; И (В) ПРИНИМАЕТЕ НАСТОЯЩЕЕ СОГЛАШЕНИЕ И СОГЛАШАЕТЕСЬ, ЧТО ВЫ ЮРИДИЧЕСКИ СВЯЗАНЫ ЕГО УСЛОВИЯМИ.

ОБЩИЕ СВЕДЕНИЯ

(A) Поставщик может обрабатывать Персональные данные от имени Клиента с целью предоставления инструментов для корпоративного соблюдения GDPR.
(B) Настоящее Соглашение об обработке персональных данных (Соглашение) устанавливает дополнительные положения, требования и условия, на которых Поставщик будет обрабатывать Персональные данные от имени Клиента. Настоящее Соглашение содержит обязательные пункты, требуемые Статьей 28(3) Общего регламента по защите данных ((EU) 2016/679) для договоров между контролерами и обработчиками.

СОГЛАСОВАННЫЕ УСЛОВИЯ

1. Определения и толкования

В настоящем Соглашении применяются следующие определения и правила толкования.

1.1. Определения:

Уполномоченные лица: лица или категории лиц, которых Клиент уполномочивает давать Поставщику письменные инструкции по обработке персональных данных через Регистрационный e-mail и от которых Поставщик соглашается исключительно принимать такие инструкции.

Бизнес-цели: услуги, которые должны быть предоставлены Поставщиком Клиенту, как описано в Генеральном соглашении, и любые другие цели, специально указанные в ПРИЛОЖЕНИИ А.

Контролирующий орган: Надзорный орган одной из стран ЕС, определенный Клиентом как Ведущий надзорный орган.
Контролер, Процессор, субъект данных, персональные данные, нарушение персональных данных и обработка: имеют значения, указанные в законодательстве о защите данных.

Законодательство о защите данных: все применимые законы о защите данных и конфиденциальности, действующие время от времени в Европе, включая, без ограничений, Общий регламент о защите данных ((EU) 2016/679) (GDPR).

Субъект данных: идентифицированное или поддающееся идентификации живое лицо, к которому относятся персональные данные.

ЕЭЗ: Европейская экономическая зона.

Персональные данные: означает любую информацию, касающуюся идентифицированного или поддающегося идентификации живого лица, которая обрабатывается Поставщиком от имени Клиента в результате или в связи с предоставлением услуг по Генеральному соглашению; поддающееся идентификации живое лицо - это лицо, которое может быть идентифицировано, прямо или косвенно, в частности, путем ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор или на один или несколько факторов, характерных для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности лица.

Обработка, процессы, обработанные, процесс: любая деятельность, которая связана с использованием Персональных данных. Она включает, но не ограничивается любой операцией или набором операций, которые выполняются над Персональными данными или наборами Персональных данных, будь то автоматизированными средствами, такими как сбор, запись, организация, структурирование, хранение, адаптация или изменение, извлечение, консультирование, раскрытие путем передачи, распространения или иного предоставления доступа, выравнивание или комбинирование, ограничение, стирание или уничтожение. Обработка также включает в себя передачу Персональных данных третьим сторонам.

Нарушение безопасности персональных данных: нарушение безопасности, приводящее к случайному, несанкционированному или незаконному уничтожению, потере, изменению, раскрытию персональных данных или доступу к ним.

Процессор: физическое или юридическое лицо, государственный орган, агентство или другой орган, который обрабатывает персональные данные по поручению Контролера.

Трансграничная передача персональных данных – передача персональных данных из территории Европейского союза за его пределы.

Записи: имеет значение, данное ему в пункте 12.

Регистрационный e-mail: e-mail, используемый для создания учетной записи на веб-сервисе Defendocs https://gdpr.itprovide.pro/

Срок: срок действия настоящего Соглашения, определенный в п. 10.

1.2. Приложения являются частью настоящего Соглашения и будут иметь силу, как если бы они были полностью изложены в тексте настоящего Соглашения. Любая ссылка на настоящее Соглашение включает Приложения.

2. Категории персональных данных и цели обработки:

2.1. Клиент и Поставщик соглашаются и признают, что для целей законодательства о защите данных:

(a) Клиент является Контролером, а Поставщик - Процессором.
(b) Клиент сохраняет контроль над Персональными данными и остается ответственным за свои обязательства по соблюдению законодательства о защите данных, включая, но не ограничиваясь, предоставление любых необходимых уведомлений и получение любых необходимых согласий, а также за письменные инструкции по обработке, которые он дает Поставщику.
(c) ПРИЛОЖЕНИЕ A описывает предмет, продолжительность, характер и цель обработки, а также категории Персональных данных и типы Субъектов данных, в отношении которых Поставщик может обрабатывать Персональные данные для достижения бизнес-целей.

3. Обязательства Поставщика

3.1. Поставщик будет обрабатывать персональные данные только в том объеме и таким образом, которые необходимы для достижения бизнес-целей в соответствии с письменными инструкциями Клиента. Поставщик не будет обрабатывать Персональные данные для любой другой цели или способом, который не соответствует настоящему Соглашению или Законодательству о защите данных. Поставщик должен незамедлительно уведомить Клиента, если, по его мнению, инструкции Клиента не соответствуют Законодательству о защите данных.

3.2. Поставщик должен незамедлительно выполнять любые письменные инструкции Клиента, требующие от Поставщика изменить, передать, удалить или иным образом обработать Персональные данные, или остановить, смягчить или устранить любую несанкционированную обработку.

3.3. Поставщик будет поддерживать конфиденциальность Персональных данных и не будет раскрывать Персональные данные третьим лицам, за исключением случаев, когда Клиент или настоящее Соглашение специально разрешают раскрытие, или в соответствии с требованиями внутреннего законодательства или законодательства ЕС, суда или контролирующего органа. Если внутреннее законодательство или законодательство ЕС, суд или контролирующий орган требует от Поставщика обрабатывать или раскрывать Персональные данные третьим лицам, Поставщик должен сначала проинформировать Клиента о таком юридическом или нормативном требовании и предоставить Клиенту возможность возразить или оспорить требование, если только внутреннее законодательство или законодательство ЕС не запрещает направление такого уведомления.

3.4. Поставщик будет разумно помогать Клиенту, без дополнительных затрат для Клиента, в выполнении обязательств Клиента по соблюдению законодательства о защите данных, принимая во внимание характер обработки данных Поставщиком и информацию, доступную Поставщику, в том числе в отношении прав Субъекта данных, оценки воздействия защиты данных и отчетности и консультаций с надзорным органом или другим соответствующим регулирующим органом в соответствии с законодательством о защите данных.

3.5. Поставщик обязан незамедлительно уведомить Клиента о любых изменениях в законодательстве о защите данных, которые могут быть обоснованно истолкованы как негативно влияющие на настоящее Соглашение.

4. Работники Поставщика

4.1. Поставщик обеспечит, чтобы все его работники:

(a) были проинформированы о конфиденциальном характере Персональных данных и связаны письменными обязательствами о конфиденциальности и ограничениями на использование Персональных данных;

(b) были осведомлены как об обязанностях Поставщика, так и о своих личных обязанностях и обязательствах в соответствии с Законодательством о защите данных и настоящим Соглашением.

4.2. Поставщик предпримет разумные шаги для обеспечения надежности, целостности и благонадежности всех работников Поставщика, имеющих доступ к Персональным данным.

5. Безопасность

5.1. Поставщик должен всегда применять соответствующие технические и организационные меры против случайной, несанкционированной или незаконной обработки, доступа, копирования, изменения, воспроизведения, отображения или распространения Персональных данных, а также против случайной или незаконной потери, уничтожения, изменения, раскрытия или повреждения Персональных данных, включая, но не ограничиваясь этим, меры безопасности, изложенные в ПРИЛОЖЕНИИ B.

5.2. Поставщик должен применять такие меры для обеспечения уровня безопасности, соответствующего соответствующему риску, в том числе по мере необходимости:

(a) способность обеспечить постоянную конфиденциальность, целостность, доступность и устойчивость систем и сервисов обработки;

(b) способность своевременно восстановить доступность и доступ к персональным данным в случае физического или технического инцидента; и

(c) процесс регулярного тестирования, оценки и анализа эффективности мер безопасности.

6. Нарушение безопасности персональных данных

6.1. Поставщик немедленно и в любом случае без неоправданной задержки уведомит Клиента в письменном виде на регистрационный адрес электронной почты, если ему станет известно о:

(a) утрате, непреднамеренном уничтожение или повреждении, порче или непригодности к использованию части или всех Персональных данных. Поставщик восстановит такие Персональные данные за свой счет как можно скорее.

(b) любой случайной, несанкционированной или незаконной обработке Персональных данных; или

(c) любом нарушении безопасности Персональных данных.

6.2. Если Поставщику становится известно о (a), (b) и/или (c) выше, он, без неоправданной задержки, также предоставит Клиенту следующую письменную информацию:

(a) описание характера (a), (b) и/или (c), включая категории персональных данных, входящих в сферу действия, и приблизительное количество как Субъектов данных, так и соответствующих записей персональных данных;

(b) вероятные последствия; и

(c) описание мер, принятых или предлагаемых к принятию для устранения (a), (b) и/или (c), включая меры по смягчению их возможных негативных последствий.

6.3. Сразу же после любой случайной, несанкционированной или незаконной обработки Персональных данных или Нарушения безопасности Персональных данных, стороны будут координировать друг с другом расследование данного вопроса. Кроме того, Поставщик будет разумно сотрудничать с Клиентом без дополнительных затрат для Клиента в решении Клиентом данного вопроса, включая, но не ограничиваясь этим:

(a) оказание помощи в проведении любого расследования;

(b) предоставление Клиенту физического доступа к любым затронутым объектам и операциям;

(c) содействие в проведении интервью с работниками Поставщика, бывшими работниками и другими лицами, имеющими отношение к данному вопросу, включая, но не ограничиваясь, его должностных лиц и директоров;

(d) предоставление всех соответствующих записей, журналов, файлов, отчетов по данным и других материалов, необходимых для соблюдения всех требований законодательства о защите данных или иным образом обоснованно требуемых Клиентом; и

(e) принятие разумных и оперативных мер по смягчению последствий и минимизации любого ущерба, возникшего в результате нарушения безопасности Персональных данных или случайной, несанкционированной или незаконной обработки Персональных данных.

6.4. Поставщик не будет информировать третьих лиц о случайной, несанкционированной или незаконной обработке всех или части Персональных данных и/или Нарушении безопасности Персональных данных без предварительного получения письменного согласия Клиента, за исключением случаев, когда этого требует внутреннее законодательство или законодательство ЕС.

6.5. Поставщик соглашается, что Клиент имеет исключительное право определять:

(a) предоставлять ли уведомление о случайной, несанкционированной или незаконной обработке и/или Нарушении безопасности Персональных данных Субъектам данных, надзорному органу, другим регуляторам, входящим в сферу действия, правоохранительным органам или другим лицам, как того требует закон или постановление или по усмотрению Клиента, включая содержание и способ доставки уведомления; и

(b) предложить ли какое-либо средство правовой защиты пострадавшим Субъектам данных, включая характер и объем такого средства правовой защиты.

6.6. Поставщик покроет все разумные расходы, связанные с выполнением обязательств по п. 6.1 - п. 6.3, за исключением случаев, когда вопрос возник в результате специальных письменных инструкций Клиента, халатности, преднамеренного невыполнения или нарушения настоящего Соглашения, в этом случае все разумные расходы покроет Клиент.

6.7. Поставщик также возместит Клиенту фактические разумные расходы, понесенные Клиентом при реагировании на случайную, несанкционированную или незаконную обработку и/или Нарушение персональных данных в той степени, в которой это произошло по вине Поставщика, включая все расходы на уведомление и любое средство правовой защиты, как указано в пункте 6.5.

7. Трансграничная передача персональных данных

7.1. Трансграничная передача персональных данных может осуществляться в случае, когда Клиент вносит Персональные данные в веб-сервис Defendocs непосредственно с территории Европейского Союза.

7.2. Внесение Клиентом Персональных данных в веб-сервис Defendocs из территории Российской Федерации или иной другой территории, за пределами Европейского Союза не является трансграничной передачей персональных в толковании настоящего Соглашения.

7.3. Клиент соглашается с тем, что при наличии трансграничной передачи Поставщик может обрабатывать персональные данные в Российской Федерации при условии соблюдения соответствующих гарантий согласно статье 46 (2) (c) - GDPR Стандартные положения о защите данных, принятые Европейской Комиссией (SCC).

8. Субподрядчики

8.1. Клиент соглашается с тем, что Поставщик будет привлекать субподрядчиков для обработки Персональных данных.

8.2. Поставщик будет привлекать субподрядчиков для обработки Персональных данных только в том случае, если Клиенту будет предоставлена возможность возразить против назначения каждого субподрядчика в течение 10 рабочих дней после того, как Поставщик предоставит Клиенту полную информацию в письменном виде по адресу регистрационной электронной почты о таком субподрядчике;

8.3. Субподрядчики, утвержденные на момент начала действия настоящего Соглашения, указаны в ПРИЛОЖЕНИИ А. Поставщик должен перечислить всех утвержденных субподрядчиков в Приложении А и указать имя и местонахождение любого субподрядчика, а также контактную информацию лица, ответственного за соблюдение конфиденциальности и защиты данных.

9. Жалобы, запросы субъектов данных и права третьих лиц

9.1. Поставщик должен без дополнительных затрат для Клиента принять такие технические и организационные меры, которые могут быть уместны, и незамедлительно предоставить Клиенту такую информацию, которую Клиент может обоснованно потребовать, чтобы позволить Клиенту соблюдать:

(a) права Субъектов данных в соответствии с Законодательством о защите данных, включая, но не ограничиваясь, права субъекта доступа, права на исправление, перенос и стирание персональных данных, возражение против обработки и автоматизированной обработки персональных данных, а также ограничение обработки персональных данных; и

(b) информацию или уведомления об оценке, направленные Клиенту надзорным органом в соответствии с Законодательством о защите данных.

9.2. Поставщик должен немедленно уведомить Клиента в письменном виде по адресу регистрационной электронной почты, если он получает любую жалобу, уведомление или сообщение, которое прямо или косвенно относится к обработке Персональных данных или к соблюдению одной из сторон Законодательства о защите данных.

9.3. Поставщик должен уведомить Клиента в течение 3 дней, если он получает запрос от Субъекта данных на доступ к его Персональным данным или на осуществление любого из его других прав в соответствии с Законодательством о защите данных.

9.4. Поставщик предоставит Клиенту, без дополнительных затрат для Клиента, свое полное сотрудничество и помощь в ответе на любую жалобу, уведомление, сообщение или запрос Субъекта данных.

9.5. Поставщик не должен раскрывать Персональные данные любому Субъекту данных или третьей стороне, кроме как в соответствии с письменными инструкциями Клиента или в соответствии с требованиями внутреннего законодательства или законодательства ЕС.

10. Срок и прекращение действия

10.1. Настоящее Соглашение будет оставаться в силе и действии до тех пор, пока деловые отношения между Клиентом и Поставщиком сохраняются

11. Возврат и уничтожение данных

11.1. По запросу Клиента, Поставщик предоставит Клиенту или третьей стороне, назначенной Клиентом в письменном виде, копию или доступ ко всем или части Персональных данных, находящихся в его владении или под его контролем, в формате и на носителях, разумно указанных Клиентом.

11.2. При прекращении Генерального соглашения по любой причине или истечении его срока, Поставщик безопасно удалит или уничтожит, или, по письменному указанию Клиента, вернет и не сохранит все или любые Персональные данные, связанные с настоящим Соглашением, находящиеся в его владении или под его контролем.

11.3. Если какой-либо закон, постановление или правительственный или регулирующий орган требует от Поставщика сохранить какие-либо документы, материалы или Персональные данные, которые Поставщик в противном случае должен был бы вернуть или уничтожить, он уведомит Клиента в письменной форме о таком требовании сохранения, предоставив подробную информацию о документах, материалах или Персональных данных, которые он должен сохранить, правовое основание для такого сохранения, и установив конкретные сроки удаления или уничтожения после того, как требование сохранения закончится.

11.4. По запросу Поставщик письменно подтвердит Клиенту, что он удалил или уничтожил Персональные данные.

12. Аудит

12.1. Поставщик разрешит Клиенту и его представителям третьей стороны проводить аудит соблюдения Поставщиком своих обязательств по Соглашению, по крайней мере, за 30 дней до уведомления, в течение Срока. Поставщик предоставит Клиенту и его представителям третьей стороны всю необходимую помощь для проведения таких аудитов без дополнительной платы для Клиента. Помощь может включать, но не ограничиваться:

(a) физический доступ, удаленный электронный доступ и копии Записей и любой другой информации, хранящейся в помещениях Поставщика или в системах, хранящих Персональные данные;

(b) доступ и встречи с любым персоналом Поставщика, разумно необходимые для предоставления всех объяснений и эффективного проведения аудита; и

12.2. Если происходит или происходило нарушение персональных данных, или Поставщику становится известно о нарушении любого из его обязательств по данному Соглашению или любого из Законодательства о защите данных, Поставщик будет:

(a) незамедлительно проведет собственную проверку для определения причины;

(b) подготовить письменный отчет, включающий подробные планы по устранению любых недостатков, выявленных в ходе аудита;

(c) предоставить Клиенту копию письменного отчета об аудите; и

(d) устранить любые недостатки, выявленные аудитом, в течение 30 дней.

12.3. Поставщик незамедлительно устранит любые исключения, отмеченные в аудиторских отчетах, путем разработки и реализации плана корректирующих действий руководством Поставщика.

13. Гарантии

13.1. Поставщик гарантирует и заявляет, что:

(a) его работники, субподрядчики, агенты и любое другое лицо или лица, имеющие доступ к Персональным данным от его имени, являются надежными и

заслуживающими доверия и прошли необходимую подготовку по Законодательству о защите данных;

(b) он и все, кто действует от его имени, будут обрабатывать Персональные данные в соответствии с Законодательством о защите данных и другими законами, постановлениями, распоряжениями, приказами, стандартами и другими аналогичными документами;

(c) у него нет оснований полагать, что Законодательство о защите данных препятствует ему предоставлять какие-либо услуги по договору Генерального соглашения; и

(d) учитывая текущую технологическую среду и затраты на реализацию, он примет соответствующие технические и организационные меры для предотвращения случайной, несанкционированной или незаконной обработки Персональных данных, а также потери или повреждения Персональных данных, и обеспечит уровень безопасности, соответствующий:

i. вред, который может возникнуть в результате такой случайной, несанкционированной или незаконной обработки, а также потери или повреждения;

ii. характер защищаемых Персональных данных; и

iii. (соблюдать все применимое законодательство о защите данных и свою политику в области информации и безопасности, включая меры безопасности, требуемые в пункте 5.1.

13.2. Клиент гарантирует и заявляет, что предполагаемое использование Поставщиком Персональных данных в Бизнес-целях и в соответствии с конкретными указаниями Клиента будет соответствовать Законодательству о защите данных.

14. Коммуникация

Все уведомления по настоящему Соглашению должны быть составлены в письменной форме и считаются надлежащим образом переданными в момент отправки, если они переданы по электронной почте.

ПРИЛОЖЕНИЕ А Цели и детали обработки персональных данных

Предмет обработки:
Облачный сервис, предлагающий клиентам инструменты для корпоративного соблюдения GDPR.

Продолжительность обработки:
В течение срока действия соглашения об обработке данных.

Категории персональных данных:

- личные данные, включая любую информацию, которая идентифицирует субъекта данных и его личные характеристики, в том числе: имя, фамилию, контактные данные (электронная почта);
- информация о запросе субъекта данных к Клиенту, включая имя или иной идентификатор субъекта, суть запроса, историю реагирования на запрос.

Типы Субъектов данных:
субъекты данных, персональные данные которых передаются Поставщику в связи с Услугами процессора Клиентом, по указанию или от имени Клиента. Сюда входят следующие Субъекты данных:

- советники, консультанты и другие профессиональные эксперты Клиента, данные которых вносятся в веб-сервис Defendocs;
- субъекты данных Клиента, подающие запросы на реализацию своих прав по защите персональных данных, сведения которых вносятся в веб-сервис Defendocs.

Утвержденные субподрядчики:

ООО «Яндекс.Облако», ООО «ЯНДЕКС» (ОГРН: 1027700229193) 119021, Россия, Москва, ул. Льва Толстого, д. 16

ПРИЛОЖЕНИЕ В Меры безопасности

1. ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ДАННЫХ ООО "АЙТИ ПРОВАЙД"

1.1. Все данные, хранящиеся в ИТ-системах, управляются безопасно в соответствии со всеми соответствующими частями Регламента ЕС 2016/679 General Data Protection Regulation ("GDPR") и всеми другими действующими сейчас или в будущем законами, регулирующими защиту данных.
1.2. Все данные, хранящиеся в ИТ-системах, доступны только тем Пользователям, у которых есть законная необходимость в доступе.
1.3. Все данные, хранящиеся в ИТ-системах, защищены от несанкционированного доступа и обработки.
1.4. Все данные, хранящиеся в ИТ-системах, защищены от потери и повреждения.
1.5. Обо всех нарушениях безопасности, связанных с ИТ-системами или любыми хранящимися в них данными, сообщается и впоследствии расследуется отделом ИТ.

2. МЕРЫ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2.1. Все программное обеспечение, используемое в ИТ-системах (включая, помимо прочего, операционные системы, отдельные программные приложения и микропрограммы), поддерживается в актуальном состоянии, и применяются все соответствующие обновления, исправления, фиксы и другие промежуточные релизы программного обеспечения.
2.2. Если в каком-либо программном обеспечении выявлен недостаток безопасности, этот недостаток немедленно устраняется или программное обеспечение может быть изъято из ИТ-систем до тех пор, пока недостаток безопасности не будет эффективно устранен.
2.3. Никто из работников ООО "АЙТИ ПРОВАЙД" не имеет права устанавливать собственное программное обеспечение, независимо от того, поставляется ли оно на физическом носителе или загружается, без разрешения IT-менеджера. Любое программное обеспечение должно быть одобрено IT-менеджером и может быть установлено только в том случае, если такая установка не представляет риска для безопасности IT-систем и не нарушает лицензионных соглашений, предметом которых может быть данное программное обеспечение.
2.4. Регулярно создаются резервные копии всех данных, хранящихся в ИТ-системах, с интервалом не менее 1 месяца, и такие резервные копии хранятся в подходящем месте на территории и за ее пределами.

3. МЕРЫ АНТИВИРУСНОЙ БЕЗОПАСНОСТИ

3.1. IT-системы ООО "АЙТИ ПРОВАЙД" (включая все компьютеры и серверы) защищены соответствующим антивирусным, брандмауэрным и другим подходящим программным обеспечением для обеспечения безопасности в Интернете. Все такое программное обеспечение поддерживается в актуальном состоянии с помощью последних обновлений и определений.
3.2. Все ИТ-системы ООО "АЙТИ ПРОВАЙД", защищенные антивирусным программным обеспечением, подвергаются полной проверке системы не реже одного раза в неделю.
3.3. Все физические носители (например, USB-накопители или диски любого типа), используемые работниками для передачи файлов, должны быть проверены на вирусы перед передачей любых файлов. Проверку на вирусы проводит менеджер по персоналу ИТ.
3.4. Работникам ООО "АЙТИ ПРОВАЙД" разрешается передавать файлы с помощью облачных систем хранения данных только с разрешения менеджера по ИТ. Все файлы,

загруженные из любой системы облачного хранения, проверяются на вирусы в процессе загрузки.

3.5. Любые файлы, отправляемые третьим лицам за пределами ООО "АЙТИ ПРОВАЙД", будь то по электронной почте, на физических носителях или другими способами (например, через общее облачное хранилище), проверяются на вирусы перед отправкой или в процессе отправки.

3.6. При обнаружении Пользователем вируса необходимо немедленно сообщить об этом в отдел информационных технологий (это правило действует даже в тех случаях, когда антивирусное программное обеспечение автоматически устраняет проблему). Отдел информационных технологий должен незамедлительно предпринять все необходимые действия для устранения проблемы. В ограниченных обстоятельствах это может включать временное удаление пострадавшего компьютера или устройства. По возможности, подходящий компьютер или устройство будет предоставлен немедленно в течение 1 дня, чтобы ограничить перебои в работе пользователя.

3.7. Все ИТ-системы с дисплеями и устройствами пользовательского ввода (например, мышь, клавиатура, сенсорный экран и т.д.) должны быть защищены, по возможности, защищенной паролем заставкой, которая активируется после 5 минут бездействия. Этот период времени не может быть изменен Пользователями, и Пользователи не могут отключить экранную заставку. Активация экранной заставки не будет прерывать или нарушать любую другую деятельность, происходящую на компьютере (например, обработку данных).

3.8. Все мобильные устройства (включая, но не ограничиваясь, ноутбуки, планшеты и смартфоны), предоставляемые Компанией, должны быть настроены на блокировку, переход в спящий режим или аналогичный режим после 5 минут бездействия, требующий пароля, кода или другой формы входа в систему для разблокировки, пробуждения или аналогичного режима. Пользователи не могут изменять этот период времени.

4. МЕРЫ БЕЗОПАСНОСТИ ОБОРУДОВАНИЯ

4.1. IT-системы ООО "АЙТИ ПРОВАЙД"расположены в помещениях, которые надежно заперты (авторизованным Пользователям предоставляется доступ с помощью смарт-карты).

4.2. Все ИТ-системы, не предназначенные для обычного использования Пользователями (включая, но не ограничиваясь, серверами, сетевым оборудованием и сетевой инфраструктурой), находятся в защищенных, климатически контролируемых помещениях в запертых шкафах, доступ к которым могут иметь только назначенные работники ИТ-отдела.

5. БЕЗОПАСНОСТЬ ДОСТУПА

5.1. Привилегии доступа ко всем ИТ-системам определяются на основе уровней полномочий работников в рамках организационной структуры компании ООО "АЙТИ ПРОВАЙД" и требований их должностных обязанностей. Работникам не предоставляется доступ к любым ИТ-системам или электронным данным, которые не являются необходимыми для выполнения их должностных обязанностей.

5.2. Все ИТ-системы (и, в частности, мобильные устройства, включая, но не ограничиваясь ими, ноутбуки, планшеты и смартфоны) защищены надежным паролем или кодом, или другой формой системы безопасного входа в систему, которую может посчитать подходящей и одобрить отдел ИТ.

5.3. Все пароли защищены с соблюдением следующих мер безопасности:

(a) Состоят как минимум из 8 символов;

(b) Содержат комбинацию заглавных и строчных букв, цифр и символов;
(c) не являются очевидными или легко угадываемыми (например, дни рождения или другие памятные даты, запоминающиеся имена, события или места и т.д.); и
(d) Созданные отдельными Пользователями.

6. БЕЗОПАСНОСТЬ ХРАНЕНИЯ ДАННЫХ

6.1. Все данные, хранящиеся в электронном виде на физических носителях, и в особенности персональные данные, надежно хранятся в запертой коробке, ящике, шкафу или аналогичном месте.
6.2. Никакие данные, в частности персональные данные, не переносятся на компьютер или устройство, лично принадлежащее работнику, за исключением случаев, когда данный работник является субпроцессором, работающим от имени ООО "АЙТИ ПРОВАЙД".

7. ЗАЩИТА ДАННЫХ

7.1. Все персональные данные (как определено в GDPR), собираемые, хранящиеся и обрабатываемые Компанией, собираются, хранятся и обрабатываются строго в соответствии с принципами GDPR.
7.2. Все Пользователи, работающие с данными от имени и по поручению Компании, должны соблюдать и постоянно выполнять меры безопасности. В частности, должно применяться следующее:
(a) Все электронные письма, содержащие персональные данные, имеют пометку "конфиденциально";
(b) Персональные данные могут передаваться только по защищенным сетям; передача по незащищенным сетям не допускается ни при каких обстоятельствах;

8. БЕЗОПАСНОСТЬ СУБПРОЦЕССОРОВ

Перед привлечением субпроцессоров ООО "АЙТИ ПРОВАЙД" проводит аудит практики безопасности и конфиденциальности субпроцессоров, чтобы убедиться, что субпроцессоры обеспечивают уровень безопасности и конфиденциальности, соответствующий их доступу к данным и объему услуг, для оказания которых они привлекаются.