Соглашение об обработке персональных данных

Соглашение об обработке персональных данных заключило Zone Media OÜ («Услугодатель»), которое является Уполномоченным обработчиком, подписано клиентом («Клиент») как Ответственным обработчиком, и является Соглашением («Соглашение»), прилагаемым к договору главного пользователя и общим условиям услуги Zone Media OÜ («Договор»). В случае противоречий между Соглашением и Договором применяются положения настоящего Соглашения.

Услугодатель

Zone Media OÜ
Рег. № 10577829
Лыытса 5, Таллинн 11415,
Эстонская Республика

_____

Арди Юргенс
член правления

Клиент

_____
_____
_____

_____
_____
_____

В связи с передачей персональных данных Клиента Услугодателю последний соглашается обрабатывать персональные данные Клиента в соответствии с условиями настоящего соглашения о неприкосновенности частной жизни и обработки персональных данных («Соглашение»), при этом Клиент и Услугодатель подтверждают, что Услугодатель не осведомлен, обрабатывает ли Клиент персональные данные в предлагаемых Услугодателем и какие данные обрабатывает.

1. Понятия

1.1. **«Инфраструктура услугодателя»** - помещения, сеть, сетевые устройства, серверы и программное обеспечение Услугодателя, которые находятся под контролем Услугодателя и согласно условиям или описанию Услуги применяются для оказания Услуги;

1.2. **«Уместные технические и организационные меры»** - процессы и процедуры, которыми, учитывая уровень развития технологии и расходы на применение, обеспечивается уместная конфиденциальность, целостность и возможность использования инфраструктуры Услугодателя.

Такие меры включают как минимум меры, установленные в Приложении 1 настоящего Соглашения **принципы инфозащиты** Zone Media OÜ, и прочие дополнительные согласованные между сторонами меры;

1.3. **«Ответственный обработчик данных»** и **«Уполномоченный обработчик данных»** - обработчик данных в понятии соответствующих правовых актов, касающихся защиты данных;

1.4. **«Правовые акты, касающиеся защиты данных»:**

(a) общее постановление о защите персональных данных в странах ЕС (постановление (ЕС) 2016/679) или иные уместные правовые акты ЕС или стран-членов ЕС.
(b) в странах, не являющихся членами ЕС – аналогичные или равноценные связанные с персональными данными законы, постановления или правила;
(c) обращаемые к исполнению руководства и инструкции, изданные местным регулирующим учреждением, отвечающим за управление правовыми актами в сфере защиты данных; и/или
(d) Изменения, исправления или дополнения, время от времени осуществляемые в документах, описанных в предыдущих пунктах (a) - (c);

1.5. **«Нарушение, связанное с персональными данными»** - нарушение установленных в общем постановлении о защите персональных данных требований безопасности, которое обусловливает случайное или незаконное уничтожение, потерю, изменение или несанкционированное разглашение передаваемых, сохраненных или иным способом обрабатываемых персональных данных или доступ к ним;

1.6. **«SO 27001»** стандарт инфозащиты ISO 27001:2014 (и вносимые в него время от времени обновления) или любой другой стандарт инфозащиты, равноценный требованиям ISO 27001:2014;

1.7. **«Персональные данные»** - имеет аналогичное значение, что и в правовых актах в сфере защиты данных;

1.8. **«Персональные данные клиента»** - персональные данные, которые загружены Клиентом на серверы Услугодателя и возникают на серверах Услугодателя при потреблении Услуги или загружены на сервер пользователями приложений Клиента и обработку которых осуществляет через услуги Услугодателя Клиент, назначенное Клиентом третье лицо или другой уполномоченный обработчик;

1.9. **«Страна, не выполняющая условия защиты данных»** - страна, не обеспечивающая адекватного уровня защиты персональных данных в понятии правовых актов в сфере защиты данные; и

1.10. **«Услуги»** - услуги, оказанные Услугодателем в связи с обработкой персональных данных Клиента и описанные в Договоре (и в производимых в нем время от времени изменениях).

1.11. Используемые в настоящем Соглашении понятия имеют аналогичное значение, что и понятия в Договоре, если не установлено иное.

2. Общее

2.1. Стороны, заявляют, что с учетом того, что Услугодатель разрешает Клиенту использовать только инфраструктуру Услугодателя для хранения данных и запуска приложений, Услугодатель не имеет представления об обрабатываемых в них данных и их типах.

2.2. Стороны подтверждают, что настоящее Соглашение является полной и окончательной документированной инструкцией по обработке персональных данных Клиента. Выполнение любых других инструкций предполагает наличие соответствующего письменного соглашения между сторонами и этому может сопутствовать дополнительная плата.

2.3. Стороны подтверждают, что Клиент является Ответственным обработчиком данных, а Услугодатель - Уполномоченным обработчиком данных. У Услугодателя нет прав на обрабатываемые Услугодателем от имени Клиента персональные данные.

2.4. Если Услугодатель или его Субподрядчик, с которым он заключил Договор обработки персональных данных от его лица, обрабатывает персональные данные, Ответственным обработчиком которых является Клиент, то Услугодатель:

(a) обрабатывает персональные данные Клиента в соответствии с правовыми актами в сфере защиты данных;
(b) не делает и не оставляет несделанным ничего, что могло бы привести к нарушению Клиентом обязательств, вытекающих из правовых актов в сфере защиты данных;
(c) Обрабатывает персональные данные Клиента только в том объеме и таким способом, которые необходимые для оказания установленных в настоящем Соглашении Услуг и в соответствии с выдаваемыми время от времени Клиентом инструкциями. Если Услугодатель нее уверен в параметрах выданных Клиентом инструкций, то Улугодатель во избежание сомнений при первой возможности обращается к Клиенту за разъяснениями и получением дальнейших инструкций;
(d) хранит персональные данные Клиента конфиденциальными, использует и разглашает их только в разрешенных в Соглашении конкретных целях;
(e) применяет уместные технические и организационные меры по защите персональных данных Клиента от несанкционированной или незаконной обработки, случайной потери, уничтожения или повреждения;
(f) на основании соответствующего ходатайства Клиента быстро возвращает Клиенту все находящиеся в его владении или под его контролем персональные данные Клиента вместе со всеми

сделанными на любом носителе копиями, если хранение копии не предусмотрено законом или договором;

(g) обеспечивает, чтобы все персональные данные Клиента, которые находятся во владении или под контролем Услугодателя, были всегда защищены надлежащим образом;

3. Изменения ситуации и законодательства

3.1. Если Услугодатель:

(a) установил, что по какой-либо причине не может исполнять вытекающие из настоящего Соглашения обязательства и не может возместить это неисполнение; или

(b) ему стало известно о каком-либо обстоятельстве или изменениях в правовых актах в сфере защиты данных, которые, по всей вероятности, существенно ухудшают способность Услугодателя исполнять вытекающие из настоящего Соглашения обязательства;

то Услугодатель информирует об этом Клиента, после чего Клиент имеет право временно приостановить обработку до реорганизации обработки способом, позволяющим устранить несоответствие. Если такая реорганизация невозможна, то Клиент имеет права прекратить обработку соответствующей части Услугодателем.

4. Субподрядчики

4.1. Клиент разрешает использовать субподрядчиков при условии, что Услугодатель несет перед Клиентом полную ответственность за действия субподрядчиков и за связанную с обработкой персональных данных деятельность или бездеятельность субподрядчиков. По требованию Услугодатель представляет список Субподрядчиков.

4.2. Услугодатель остается единственным контактным лицом Клиента по всем вопросам, входящим в сферу регулирования настоящего Соглашения, и заботится о том, чтобы его субподрядчик соблюдал обязывающие требования настоящего Соглашения так, как они применяются к Услугодателю.

4.3. Услугодатель заботится о том, чтобы все использовавшиеся им при оказании Услуги в рамках настоящего Соглашения субподрядчики исполняли обязательство конфиденциальности на условиях (и не менее ограничивающих), установленных в настоящем Соглашении.

5. Условия доступа

5.1. Услугодатель обеспечивает, чтобы доступ к персональным данным разрешался только:

(a) уполномоченным согласно требованиям чиновникам, работникам, агентам и подрядчикам («Работники Услугодателя»), которым необходим доступ к персональным данным для исполнения обязательств, вытекающих из Договора Услугодателя и настоящего Соглашения;
(b) к части или частям персональных данных, которые необходимы для исполнения обязательств работника Услугодателя.

5.2. Услугодатель обеспечивает, чтобы все работники Услугодателя:

(a) были осведомлены о конфиденциальном характере персональных данных;
(b) прошли обучение в сфере хранения, защиты и обращения с персональными данными;
(c) были осведомлены о правовых актах в сфере защиты данных и вытекающих из настоящего Соглашения обязательствах и задачах Услугодателя и работников.

5.3. Услугодатель предпринимает разумные шаги по обеспечению благонадежности работников и субподрядчиков Услугодателя, имеющих доступ к персональным данным.

6. Передача данных

6.1. Услугодатель не передает персональные данные в расположенную за пределами Европейской экономической зоны страну, не выполняющую условия Защиты данных, и не обеспечивает доступность персональных данных из страны, не выполняющей условия Защиты данных, без предварительного письменного одобрения Клиента.

6.2. Передачу персональных данных или доступ к ним для находящихся за пределами Европейской экономической зоны третьих лиц (в том числе, аффилированных предпринимателей Услугодателя), которые не находятся в стране, не исполняющей условия Защиты данных, регулирует заключенный между Услугодателем и Клиентом договор передачи данных, который содержит стандартные условия Ответственного и Уполномоченного обработчиков данных, опубликованные в решении Европейской комиссии от 5 февраля 2010 г. (решение 2010/87/EL), или иные условия аналогичных договоров, которые Европейская комиссия время от времени может принимать («Образцовые условия ЕС»).

7. Извещения и инциденты, нарушения, связанные с персональными данными

7.1. Услугодатель информирует Клиента в течение двадцати четырех (24) часов, если Услугодатель:

(a) получает от связанного с обработкой персональных данных учреждения необходимый для расследования или аудита запрос или ходатайство, за исключением случая, если это заявление закрещено для Услугодателя законом;
(b) планирует передать персональные данные какому-либо учреждению;
(c) получил ходатайство третьего лица или работника Клиента, Клиента или договорного партнера для разглашения информации, связанной с персональными данными Клиента или обработкой персональных данных Клиента;
(d) установил или имеет обоснованные подозрения, что имеет место связанное с персональными данными Нарушение.

7.2. При необходимости оказывает Клиенту Услугодателя разумную помощь в связи с инициированным работником Клиента, Клиентом, подрядчиком или учреждением требованием и/или запросом, расследованием или оценкой обработки.

7.3. В случае связанного в персональными данными Нарушения Услугодатель применяет при первой возможности адекватные компенсационные меры, в том числе, информирование Клиента о причинах нарушения, проведение расследования и представление Клиенту отчета и предложения о мерах по исправлению.

7.4. Услугодатель и Клиент сотрудничают в полном объеме для разработки и реализации плана действий, применяемого в случае связанного с персональными данными Нарушения.

7.5. Услугодатель предоставляет следующую информацию относительно связанного с персональными данными Нарушения (и обновляет ее в случае обоснованного ходатайства Клиента):

(a) Предполагаемая дата и время связанного с персональными данными Нарушения, а также дата и время, когда Услугодателю стало известно о связанном с персональными данными Нарушении;
(b) Обстоятельства, касающиеся связанного с персональными данными Нарушения, и любые факты относительно характера и объема связанного с персональными данными Нарушения;
(c) Имя и контактные данные специалиста Услугодателя по защите данных или иного контактного лица, которое может дать соответствующую дополнительную информацию;
(d) Описание вероятных последствий связанного с персональными данными Нарушения;
(e) Описание мер или предложений, примененных для устранения связанного с персональными данными Нарушения;
(f) Все детали расследования, начатого в отношении связанного с персональными данными Нарушения (внутри или вне предприятия Услугодателя (напр., регулирующее учреждение));
(g) Объем и детали жалоб, полученных от отдельных лиц относительно связанного с персональными данными Нарушения.

7.6. Услугодатель информирует Клиента о связанном с персональными данными Нарушении до информирования регулирующего учреждения и предоставляет Клиенту разумную возможность ознакомиться с информацией и дополнить ее. Клиент и Услугодатель делают все от них зависящее для уменьшения влияния связанного с персональными данными Нарушения.

7.7. По требованию Клиента Услугодатель проводит сотрудничество для адекватного информирования оказавшихся под влиянием Нарушения работников или Клиентов.

8. Вторичная обработка

8.1. Услугодатель подтверждает, что он:

(a) не проводит дополнительного расследования, анализа, профилирования и иных действий по обработке, которые включают использование какого-либо элемента персональных данных (в том числе, сводные данные) или информацию, полученную в результате обработки таких данных вне зоны применения услуг;

(b) не передает содержащие персональные данные файлы для дальнейшей обработки третьим лицам или их агентам без предварительного письменного согласия Клиента.

9. Требования безопасности

9.1. Услугодатель не делает и не оставляет несделанным ничего, что наносит ущерб или, разумно предполагая, может нанести ущерб системам или персональным данным Клиента.

9.2. Организация защиты

(a) Услугодатель назначает специального работника, отвечающего за обеспечение общепринятых норм инфозащиты во всей организации Услугодателя и в связи с оказанием Услуг, в том числе, оглашение политики по инфозащите.

(b) Руководитель по инфозащите Услугодателя несет ответственность за функционирование инфозащиты во всей организации Услугодателя.

(c) Услугодатель обеспечивает оказание Услуг в соответствии с политикой инфозащиты Услугодателя.

9.3. Управление доступом

(a) Услугодатель проверяет идентичность личности всех имеющих доступ к системе Клиента работников Услугодателя. При обоснованной необходимости Услугодатель должен сообщить Клиенту имена работников Услугодателя и необходимый и реальный уровень доступа к информации Клиента.

(b) Услугодатель обеспечивает, что установленные в предыдущем пункте обязательства поддерживают данные внутреннего аудита и

мониторинг сбоев, позволяющие активно обнаруживать и расследовать нарушения.

9.4. Физическая безопасность

(a) Услугодатель обязуется защищать персональные данные Клиента от недопустимого физического доступа и/или вызванного повреждением ущерба. Это включает контроль за физическим доступом, например, охрана зданий от несанкционированного входа (напр., применение замков, задвижек или равноценных мер для легко открываемых дверей и окон), разрешение физического доступа на критические участки только для определенных работников, для осуществляющих надзор и получивших соответствующее право доступа не работающих на предприятии лиц, защита соединений связи и носителей данных.

9.5. Контроль безопасности

(a) Услугодатель разрешает работникам Клиента, уполномоченным представителям и другим лицам, которым Клиент по закону обязан предоставлять право доступа или контроля, проверять и оценивать соответствие Услугодателя обязательствам, установленным в настоящем Соглашении. Содержанием контроля может быть также передача результатов проверки последней сертификации и аудита, напр., справка о результатах и применимости аудита сертификации ISO 27001.

(b) Исполнители указанного контроля имеют право исследовать меры и процедуры проверки рисков безопасности ИТ-систем Услугодателя и опросить работников Услугодателя, чтобы оценить соответствие вышеизложенного установленным в настоящем Соглашении обязательствам.

(c) Услугодатель имеет право потребовать за участие в контроле безопасности Клиента разумную плату, если контроль безопасности не ограничивается выдачей существующей документации или является чрезмерным по оценке Услугодателя.

10. Компенсации

10.1. Услугодатель несет ответственность за все расходы и ущерб, обусловленные несоответствием истине утверждений, приведенных в Приложении 1 настоящего Соглашения.

11. Прекращение договора

11.1. В случае прекращения договора:

(a) Услугодатель соглашается незамедлительно прекратить обработку персональных данных Клиента и при необходимости отправить все персональные данные Клиента (включая их копии) Клиенту в указанное Клиентом место;

(b) Услугодатель удаляет/уничтожает все находящиеся в его владении персональные данные Клиента способом, не допускающим восстановления персональных данных Клиента вне действующей политики архивирования или вытекающего из закона обязательства, и при необходимости передает Клиенту подтверждение Услугодателя относительно осуществления этих действий;

(c) Если удаление/уничтожение Услугодателем персональных данных Клиента запрещено законом, то Услугодатель информирует Клиента, и стороны договариваются о плане, когда и как находящиеся во владении Услугодателя персональные данные Клиента будут удалены или уничтожены.

Приложение 1
Принципы инфозащиты Zone Media OÜ

1. Общие положения

Миссия Zone заключается в предложении простых, быстрых и надежных решений для передачи информации и ее обработки в Интернете.

Инфозащита имеет критическое значение в выполнении миссии нашего предприятия, и правление и работники Zone делают все для сохранения конфиденциальности, целостности и применимости инфоресурсов предприятия и его клиентов.

Например, при обработке персональных данных мы выполняем две одинаково важных роли – в зависимости от контекста мы можем быть как **ответственным обработчиком, так и уполномоченным обработчиком персональных данных**.

В контексте общего постановления о защите персональных данных наша главная задача - применять для своих услуг и инфраструктуры (площади размещения, серверы, сетевые устройства и т. д.) достаточные технические и организационные меры безопасности, чтобы обрабатываемые клиентами данные были защищены от случайного или противозаконного удаления, неавторизованного доступа или разглашения.

В данном инфолисте мы знакомим вас с тем, что мы делаем для защиты обрабатываемых в нашей инфраструктуре данных (в т. ч. персональных данных).

Крайне важно, чтобы вы ознакомились с этим инфолистом, поскольку регуляция Европейского парламента и совета 2016/679, т. е. общее постановление о защите персональных данных отмечает следующее:

> Если персональные данные обрабатываются от имени ответственного обработчика, то ответственный обработчик использует только таких уполномоченных обработчиков, которые дают достаточную гарантию, что применяют уместные технические и организационные меры таким образом, что обработка соответствует требованиям настоящего постановления и при этом обеспечивается защита прав субъекта данных.

Ответственный обработчик – это вы. Вы должны убедиться, что мы в качестве уполномоченного обработчика защищаем свою организацию, услуги и инфраструктуру (площади размещения, техническое обеспечение, программное обеспечение, сети обмена данных и прочие ресурсы) в соответствии с требуемыми в законах и распространенными в сфере лучшими практиками. Разумеется, вы также должны знать свои задачи и ответственность при обработке персональных данных.

2. Характер услуг

Начнем с общего описания своих услуг.

Пользуясь нашими услугами, вы должны иметь в виду, что подавляющую часть наших услуг мы предлагаем клиентам в виде универсальной облачной услуги. Это означает, что они по умолчанию не адаптированы индивидуально для вас, а соответствуют общим требованиям рынка. Однако индивидуальные соглашения и адаптации все же возможны.

В качестве предприятия, предлагающего облачные услуги, у нас отсутствует контроль над тем, какие данные вы загружаете в нашу инфраструктуру или с какими данными обращаетесь. Это означает, что по умолчанию мы не знаем, пользуются ли нашими услугами для обработки персональных данных, какие персональные данные обрабатываются и является ли такая обработка законной. При необходимости вы должны сами оценить влияние обработки данных и ее соответствие действующему законодательству.

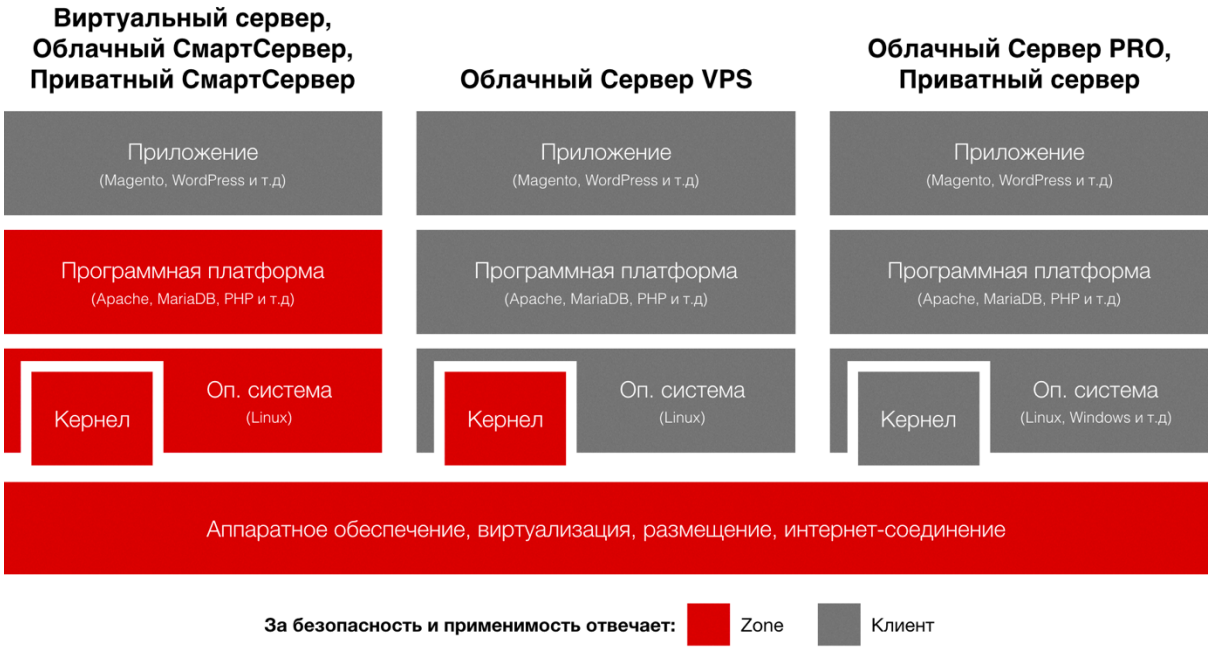
3. Классы услуг

Большинство предлагаемых Zone услуг классифицируются как облачные услуги. Они основаны на основных моделях облачных услуг:

- приложение как услуга, или «*Software as a Service*» (SaaS), доставляет клиенту уже готовое для пользования приложение;
- платформа как услуга, или «*Platform as a Service*» (PaaS), предлагает необходимые для внедрения приложения условия;
- Инфраструктура как услуга, или «*Infrastructure as a Service*» (IaaS), предлагает клиенту виртуальные серверы для создания своей платформы.

Объем задач Zone и клиента варьирует в рамках этих моделей согласно выбранной услуге. Помимо прочего, мы это описываем в инфолисте каждой нашей услуги в секции «Распределение ответственности».

Общую картину предлагает следующая схема:



Содержащиеся в услуге виртуального сервера э-почта, DNS и ZoneCloud представляют собой услугу SaaS, и ответственность Zone расширяется также на слой приложения.

Важно иметь в виду, что безопасность транспорта паролей, приложений и данных почти всегда по умолчанию находится в сфере ответственности клиента.

4. Модели реализации услуг

Применяются три модели реализации услуг:

- общее пользование;
- отдельное пользование;
- гибридное пользование.

Общее пользование означает, что одними и теми же серверами пользуются несколько организаций. На общем пользовании базируются такие услуги, как Виртуальный сервер, Облачный сервер VPS, Облачный сервер Pro и Умный облачный сервер. Эти услуги дешевле, однако с ними связано больше рисков, чем с отдельным пользованием – дополнительные риски связаны в основном с другими пользователями услугой.

Например, при общем пользовании существует возможность, что при чрезмерном потреблении ресурсов один клиент может отрицательно повлиять на возможность пользования веб-сайтами других клиентов. В предложении базирующихся на общем пользовании услуг Zone имеет долговременный опыт, и в нашей программной платформе уже встроены средства, уменьшающие такой риск, однако полностью риски, связанные с доступностью ресурсов, среде общего пользования уменьшить невозможно.

При **отдельном пользовании** серверы находятся в распоряжении только одного клиента. Отдельное пользование применяется при услугах Приватного сервера и частично Умного приватного сервера, в рамках которых клиенту гарантированно выделяются приватные серверные ресурсы. При отдельном пользовании клиент не делит серверные ресурсы с другими клиентами, что существенно уменьшает риски, связанны с применимостью услуги и конфиденциальностью данных. Отдельное пользование позволяет также при необходимости применять к серверу(ам) ориентированные на клиента меры инфозащиты.

Самое большое преимущество отдельного пользования заключается в том, что в случае возможных инцидентов приоритетным является восстановление услуги конкретному клиенту. При общем пользовании исходят из интересов большинства клиентов. Небольшим недостатком является более высокая цена за отдельное пользование.

При **гибридном пользовании** можно в компонентах услуги применять различные модели. По умолчанию гибридная модель применяется в случае Умного приватного сервера, чьи веб-приложения и базу данных обслуживающий сервер ориентирован только на одного клиента, но услуга э-почты и DNS делит ресурсы с другими клиентами. В случае специальных решений это разделение, разумеется, может варьировать – по желанию мы можем предложить также приватные серверы э-почты и т. п.

5. Инфозащита в Zone

5.1. Процесс и организация инфозащиты

Первостепенное значение имеет сосредоточенность организации на инфозащите. Для этого правление ввело на предприятии политику инфозащиты, которая применяется на всем предприятии – соблюдения установленных принципов ожидают от руководителей и работников Zone, а также подрядчиков, участвующих в работе нашего предприятия. Соответствие политики современным требованиям оценивают не реже одного раза в год.

За составление, дополнение и применение политики инфозащиты в Zone отвечает руководитель по инфозащите.

Руководителя по инфозащите в его работе поддерживают рабочая группа по инфозащите и специалист по защите персональных данных. Разумеется, в процесс инфозащиты вовлечены все структурные подразделения и работники предприятия.

Свою **политику в сфере инфозащиты** мы выстроили согласно стандарту ISO/IEC 27001:2014 и наша цель – подтвердить в будущем соответствие стандарту, пройдя официальную сертификацию.

В **управлении рисками в сфере инфозащиты** Zone исходит из рекомендаций стандарта ISO/IEC 27005:2014 и применяет основанную на ресурсах качественную методику взвешивания рисков.

5.2. **Уровень безопасности инфоресурсов клиента**

Ответственным обработчиком сохраняемых и обрабатываемых в ИТ-системах Zone инфоресурсов клиента (файлы, базы данных, э-письма и т. д.) является клиент.

Уровень безопасности инфоресурсов клиента на нашем предприятии является конфиденциальным и означает следующее: использование информации разрешается только конкретным группам пользователей, доступ к информации разрешен в случае обоснованного интереса ходатайствующего о доступе лица (например, это нужно для выполнения трудовых обязанностей).

Действующий в Zone уровень безопасности не распространяется автоматически за пределы предприятия. Клиент должен сохранять, обрабатывать и передавать свою информацию в ИТ-системах Zone в соответствии с назначенными им для своих инфоресурсов уровнями безопасности, взвешенными рисками и организовать для них применение соответствующих мер безопасности.

Мы никогда никому не продаем загруженные когда-то в инфраструктуру Zone, загруженные пользователями клиента или созданные в сервере в ходе пользования клиентом услугой данные и не используем такие данные без разрешения клиента в своих непосредственных экономических целях. Zone обрабатывает такие данные только в объеме, необходимом для предложения своих услуг или связанной с ними пользовательской поддержки.

5.3. **Защита персональных данных в Zone**

Для осуществления надзора за защитой персональных данных мы создали роль специалиста по защите данных, исполнитель которой прошел акцептируемую Инспекцией по защите данных программу обучения.

Мы ведем учет как обрабатываемых персональных данных, так и влияния обработки на эти данные.

Подробнее об обработке персональных данных можно прочитать в **Уведомлении о приватности Zone Media OÜ.**

5.4. **Местонахождение данных**

Мы оказываем свои услуги в физически безопасных условиях. Применяемые Zone центры данных находятся на территории Европейского союза.

Наша инфраструктура с целью уменьшения рисков инфозащиты, рисков сохранности и бизнес-рисков, а также предложения клиентам уникальных возможностей распределена по 5 центрам данных, 4 из которых находятся в Эстонии, в Таллинне, и 1 находится в Голландии, в Амстердаме. При размещении инфраструктуры Zone сотрудничает с такими признанными партнерами, как Equinix, Linxtelecom, Telia и Elisa.

Применяемые Zone центры данных находятся в зданиях, построенных или специально приспособленных для размещения устройств информационно-коммуникационной технологии и изолированы от общественных помещений. Устройства расположены в центрах данных на изолированной защитным

ограждением площади или в запертых шкафах. Доступ ограничен лицами, которым он необходим в связи с их трудовыми обязанностями.

Центра данных оснащены камерами видеонаблюдения и охранной сигнализацией, относительно входа в центры ведутся логи. Применяются автоматическая пожарная сигнализация и автоматическая система газотушения.

Для поддержания температуры и относительной влажности воздуха на нужном для серверов и устройств обмена данных уровне все центры данных оснащены устройствами и системами охлаждения.

Для обеспечения более надежного электроснабжения все устройства Zone подключены к источникам буферного питания (UPS), здания оснащены электрогенераторами.

Для обеспечения возможности пользования во всех центрах данных применяется избыточность устройств и технических систем.

Территориям, где находятся используемые Zone здания, не угрожают опасности, обусловленные погодными условиями или местной геологией, до сих пор они не причиняли ущерба центрам данных.

5.5. **Обмен данными**

Для уменьшения связанных с обменом данными рисков инфозащиты, рисков сохранности и бизнес-рисков, а также с целью предложения клиентам уникальных возможностей Zone сотрудничает со многими надежными телекоммуникационными предприятиями. Партнерами Zone по обмену данными являются Cogent Communications, Level3 Communications, Linxtelecom, Telia и Elisa.

В Эстонии Zone параллельно использует три, а в Голландии два транзитных интернет-соединения – избыточность соединений обеспечивает клиентам подключение также в случае одиночного нарушения соединения или во время работ по обслуживанию.

Между центрами размещений Эстонии Zone построил уникальную приватную региональную сеть, цель которой – дополнительно уменьшить обусловленные внешними факторами риски для возможности пользования услугами. Оказывающие серверные услуги центры данных одновременно соединены с двумя другими центрами – образовавшийся в результате сетевой круг позволяет сохранять в центре подключение также при неисправности одного соединения или во время работ по обслуживанию.

Со многими эстонскими телекоммуникационными предприятиями и предприятиями, предлагающими интернет-услуги, Zone также соединен с помощью двух крупнейших прямых соединительных узлов эстонского Интернета - TLLIX и RTIX.

Zone заботится о том, чтобы в нормальной ситуации соединения обмена данными работали с неполной нагрузкой и дополнительные ресурсы были быстро доступны.

Для уменьшения рисков, обусловленных специфическими атаками на услуги, интернет-соединения Zone оснащены специальными устройствами, уменьшающими отрицательное воздействие атак.

5.6. **Архивирование данных**

Zone делает резервные копии с серверов, связанных с управляемыми Zone услугами, согласно следующим правилам:

- резервную копию расположенных на веб-серверах файлов, баз данных SQL и почтовых ящиков нужно делать не реже одного раза в день;
- резервную копию должно быть возможно использовать для восстановления архивированных данных как минимум в течение 14 дней с момента создания резервной копии;
- при необходимости резервные копии нужно делать перед крупными программными обновлениями или изменениями, которые могут угрожать целостности данных.

Резервные копии с серверов, применяемых для предложения управляемых Zone услуг, мы храним отдельно от производственной среды.

В случае базирующихся на отдельном пользовании услуг можно адаптировать политику архивирования к потребностям клиента.

Как клиент вы должны учитывать, что время восстановления данных непосредственно зависит от характера и объема данных, а в случае общего пользования и от других использующих этот же ресурс клиентов.

5.7. **Мониторинг**

Zone наблюдает за работой оказывающих услуги серверов 24 часа в сутки и 7 дней в неделю.

В частности Zone отслеживает ссылки на компрометацию платформы или услуг клиентов, в т. ч. запуск неизвестных процессов, неожиданное открытие сетевых портов, активность пользователей, оправление спама и т. д.

Активный мониторинг осуществляется по будним дням в 08.30-17.30, во время активного мониторинга работники Zone Media отслеживают выход системы мониторинга в реальном времени, система мониторинга информирует техников Zone также посредством сети мобильной связи. Реагирование на инциденты происходит немедленно.

Пассивный мониторинг проводится по будним дням в 17.30-08.30 и по выходным круглосуточно, во время пассивного мониторинга система мониторинга информирует дежурного техника Zone о проблемах посредством сети мобильной связи. Дежурный техник реагирует на инциденты незамедлительно.

5.8. **Клиентская поддержка**

Телефонная поддержка Zone и поддержка по э-почте работают по будним дням в 09.00 – 17.00 (часовой пояс EET/EEST).

Телефон клиентской поддержки: +372 688 6886
Э-почта клиентской поддержки: info@zone.ee

По вопросам, касающимся обработки персональных данных, можно обращаться непосредственно к специалисту Zone по защите данных по адресу dataprotection@zone.ee.

Состояние сервисной платформы Zone отражается на сайте **http://status.zone.eu.**

Принятой в нерабочее время э-почтой занимается дежурная команда, организующая реагирование на критические инциденты.

Для клиентов услуг отдельного пользования при необходимости доступен 24/7 номер дежурного телефона, предусмотренный для информирования о критических инцидентах.

5.9. Привлеченные Zone уполномоченные обработчики

Для обработки клиентских данных мы можем привлекать уполномоченных обработчиков.

Мы делаем это, если достаточно уверены в том, что они применяют уместные технические и организационные меры способом, обеспечивающим соответствие обработки данных представленным в соответствующих законах требованиям.

Список привлеченных к обработке клиентских данных важных уполномоченных обработчиков мы публикуем на своем сайте (https://www.zone.ee).