Приложение об аутсорсинге обработки данных в соответствии со ст. 28 GDPR к контракту №:

**Подрядчик (наименование, адрес, страна):**

# Содержание

* Оговорки с 1 по 11
* Приложение I. Описание обработки
* Приложение II – Список субподрядчиков
* Приложение III – Технические и организационные меры (ТОМ)

# Пункт 1. Цель и область применения

1. Целью настоящего Приложения по [заключению субконтракта на выполнение работ внешними фирмами](https://www.multitran.com/m.exe?s=%D0%B7%D0%B0%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BD%D0%B8%D0%B5+%D1%81%D1%83%D0%B1%D0%B4%D0%BE%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%B0+%D0%BD%D0%B0+%D0%B2%D1%8B%D0%BF%D0%BE%D0%BB%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5+%D1%80%D0%B0%D0%B1%D0%BE%D1%82+%D1%81+%D0%B2%D0%BD%D0%B5%D1%88%D0%BD%D0%B8%D0%BC%D0%B8+%D1%84%D0%B8%D1%80%D0%BC%D0%B0%D0%BC%D0%B8&l1=2&l2=1) по обработке данных (Оговорки) является обеспечение соблюдения статьи 28(3) и (4) Регламента (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и свободного перемещения таких данных (**Общий регламент по защите данных).**
2. GIZ в качестве контролера и подрядчик в качестве обработчика (Стороны) согласились с настоящими Оговорками, чтобы обеспечить соблюдение Статей 28(3) и (4) Регламента (ЕС) 2016/679.
3. Настоящие Оговорки применяются к обработке персональных данных, как указано в Приложении I.
4. Приложения I–III являются неотъемлемой частью настоящих Оговорок.
5. Настоящие Оговорки не наносят ущерба обязательствам, которым подчиняется GIZ в соответствии с Регламентом (ЕС) 2016/679.
6. Настоящие Оговорки сами по себе не обеспечивают соблюдение обязательств, связанных с международными переводами в соответствии с Главой V Регламента (ЕС) 2016/679. Если происходит передача персональных данных от GIZ подрядчику в третьей стране, для такой передачи данных требуется юридическое основание. Если передача не может быть основана на решении об адекватности в соответствии со статьей 45 Регламента (ЕС) 2016/679 или соответствующих гарантиях в соответствии со статьей 46 Регламента (ЕС) 2016/679 и ни одно из отступлений для конкретных ситуаций в соответствии со Статьей 49 Регламента (ЕС) 2016/679 не применимо, между GIZ и подрядчиком должно быть заключено юридически обязывающее соглашение для установления правовой основы. Соглашение должно быть заключено путем заключения стандартных положений о защите данных в соответствии со статьей 46(1) и пунктом (c) статьи 46(2) Регламента (ЕС) 2016/679.

# Пункт 2. Неизменность оговорок.

Стороны обязуются не изменять Оговорки, за исключением дополнения информации в Приложениях или обновления информации в них. Изменения и дополнения информации, содержащейся в Приложениях, не требуют письменного оформления контракта и могут быть согласованы в текстовой форме.

# Пункт 3 – Интерпретация

1. Если в этих Оговорках используются термины, определенные в Регламенте (ЕС) 2016/679 соответственно, эти термины имеют то же значение, что и в этом Регламенте.
2. Настоящие Оговорки должны читаться и интерпретироваться в свете положений Регламента (ЕС) 2016/679.
3. Настоящие Оговорки не должны интерпретироваться таким образом, который противоречит правам и обязанностям, предусмотренным Регламентом (ЕС) 2016/679, или таким образом, который наносит ущерб основным правам или свободам субъектов данных.

# Пункт 4. Иерархия

В случае противоречия между настоящими Оговорками и положениями связанных с ними контрактов между Сторонами, существовавшими на момент согласования или заключения настоящих Оговорок в дальнейшем, эти Оговорки имеют преимущественную силу.

# Пункт 5. Описание обработки

Подробности операций по обработке, в частности категории персональных данных и цели обработки, для которых персональные данные обрабатываются от имени GIZ, указаны в Приложении I.

# Пункт 6. Обязанности сторон

* 1. **Инструкции**

1. Подрядчик должен обрабатывать персональные данные только по документально оформленным инструкциям GIZ, если только этого не требует законодательство Союза или государства-члена, которому подчиняется обработчик. В этом случае подрядчик должен проинформировать GIZ об этом юридическом требовании перед обработкой, если только закон не запрещает это по важным причинам, представляющим общественный интерес. Последующие инструкции также могут даваться GIZ на протяжении всего периода обработки персональных данных. Инструкция — это письменный, электронный или устный приказ GIZ, направленный на конкретную обработку данных подрядчиком. Мероприятия должны быть задокументированы. Инструкции сначала определяются техническим заданием, а затем могут быть изменены, дополнены или заменены GIZ в документированной форме отдельной инструкцией.
2. Подрядчик должен немедленно проинформировать GIZ, если, по его мнению, инструкции GIZ нарушают Регламент (ЕС) 2016/679 или применимые положения Союза или государства-члена ЕС о защите данных.
3. GIZ может в любое время запросить отказ, исправление, адаптацию, удаление и ограничение обработки данных.
4. Подрядчик может предоставлять информацию третьим лицам или субъекту данных только с предварительного явного согласия GIZ. Согласие должно быть подтверждено подрядчиком документально.

# Цель ограничения

Подрядчик должен обрабатывать персональные данные только для конкретных целей обработки, как указано в Приложении I, если он не получит дальнейших указаний от GIZ.

# Продолжительность обработки персональных данных

Обработка подрядчиком осуществляется только в течение периода, указанного в Приложении I.

# Безопасность обработки

1. Подрядчик должен как минимум реализовать технические и организационные меры, указанные в Приложении III, для обеспечения безопасности персональных данных. Это включает в себя защиту данных от нарушения безопасности, ведущего к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к данным (нарушение персональных данных). При оценке соответствующего уровня безопасности Стороны должным образом учитывают современное состояние, затраты на внедрение, характер, объем, контекст и цели обработки, а также риски, связанные с субъектами данных.
2. Благодаря техническому прогрессу подрядчику разрешено применять альтернативные адекватные меры. Это не должно опускаться ниже уровня мер безопасности, изложенных в Приложении III. Значительные изменения должны быть задокументированы.
3. Подрядчик предоставляет доступ к обрабатываемым персональным данным членам своего персонала только в той мере, в которой это строго необходимо для реализации, управления и мониторинга контракта. Подрядчик должен обеспечить, чтобы лица, уполномоченные обрабатывать полученные персональные данные, взяли на себя обязательство соблюдать конфиденциальность или находились под соответствующим установленным законом обязательством по соблюдению конфиденциальности.

# Чувствительные данные

Если обработка включает в себя персональные данные, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения или членство в профсоюзе, генетические данные или биометрические данные с целью однозначной идентификации физического лица, данные, касающиеся здоровья или сексуальной жизни или сексуальной ориентации человека или данные, касающиеся уголовных судимостей и правонарушений («конфиденциальные данные»), подрядчик должен применить конкретные ограничения и/или дополнительные меры защиты. Это может включать, например, ограничение персонала, имеющего доступ к персональным данным, или обеспечение работоспособности, конфиденциальности, целостности, доступности и устойчивости систем и услуг.

# Документация и соблюдение требований

1. Подрядчик должен оперативно и адекватно реагировать на запросы GIZ об обработке данных в соответствии с настоящими Оговорками.
2. По запросу GIZ подрядчик должен предоставить GIZ информацию, необходимую GIZ для ведения учета деятельности по обработке в значении статьи 30(1) Регламента (ЕС) 2016/679.
3. Подрядчик должен немедленно информировать GIZ о любых проверках и мерах, принятых надзорными органами, а также о том, что надзорный орган запрашивает, расследует или получает другие запросы от подрядчика в пределах своей ответственности.
4. Подрядчик должен предоставить GIZ всю информацию, необходимую для демонстрации соблюдения обязательств, изложенных в настоящих Оговорках и ​​вытекающих непосредственно из Регламента (ЕС) 2016/679. По запросу GIZ подрядчик также должен разрешить и способствовать аудиту деятельности по обработке, предусмотренной настоящими Оговорками, через разумные промежутки времени или при наличии признаков несоблюдения требований. Принимая решение о проверке или аудите, GIZ может принять во внимание соответствующие сертификаты, имеющиеся у подрядчика.
5. GIZ может провести аудит самостоятельно или поручить независимому аудитору. Аудит может также включать проверки помещений или физических объектов подрядчика и, при необходимости, проводится с заблаговременным уведомлением.
6. Стороны предоставляют информацию, указанную в настоящей Оговорке, включая результаты любых проверок, доступную компетентному надзорному органу по запросу.

# Пункт 7 – Использование субподрядчика

1. Подрядчик не имеет права передавать субподрядчику (другому обработчику) какие-либо операции по обработке, выполняемые от имени GIZ в соответствии с настоящими Оговорками, без предварительного специального документально подтвержденного письменного разрешения GIZ. Подрядчик должен подать запрос на получение специального разрешения не менее чем за 20 календарных дней до предполагаемого привлечения соответствующего субподрядчика вместе с информацией, необходимой для того, чтобы GIZ могло принять решение о разрешении. Информация включает как минимум полное имя, включая адрес и страну субподрядчика, а также описание обработки субподрядчиком (включая предмет, характер и продолжительность). GIZ соглашается на привлечение субподрядчиков, указанных в Приложении II. Стороны будут поддерживать Приложение II в актуальном состоянии.
2. Если привлечение субподрядчиков (других обработчиков) исключено, это указано GIZ в Приложении II.
3. Если подрядчик привлекает субподрядчика для выполнения конкретных действий по обработке (от имени GIZ), он должен сделать это посредством контракта, который налагает на субподрядчика как минимум те же обязательства по защите данных, что и те, которые возлагаются на подрядчика в соответствии с настоящими Оговорками. Подрядчик должен гарантировать, что субподрядчик соблюдает обязательства, которым подчиняется подрядчик в соответствии с настоящими Оговорками и Регламентом (ЕС) 2016/679.
4. По запросу GIZ подрядчик должен предоставить GIZ экземпляр такого договора субподряда и всех последующих изменений. В той мере, в какой это необходимо для защиты коммерческой тайны или другой конфиденциальной информации, включая персональные данные, подрядчик может отредактировать текст соглашения до предоставления экземпляра.
5. Подрядчик несет полную ответственность перед GIZ за выполнение обязательств субподрядчика в соответствии с его контрактом с подрядчиком. Подрядчик должен уведомить GIZ о любом невыполнении субподрядчиком своих контрактных обязательств. В этом случае по требованию GIZ подрядчик должен полностью или частично прекратить трудовые отношения с субподрядчиком или расторгнуть договорные отношения с ним, если и в той мере, в которой это не является несоразмерным.
6. Субподряд в значении настоящих Оговорок не включает услуги, которые подрядчик использует у третьих лиц в качестве вспомогательных услуг для поддержки выполнения заказа, например, телекоммуникационные услуги. Однако подрядчик обязан заключить соответствующие и юридически обязывающие договорные соглашения и принять соответствующие меры проверки для обеспечения защиты данных и безопасности данных GIZ, даже в случае привлечения сторонних вспомогательных услуг.
7. Подрядчик должен согласовать с субподрядчиком Оговорку о третьей стороне-бенефициаре, согласно которой в случае, если подрядчик фактически исчез, прекратил свое существование по закону или стал неплатежеспособным, GIZ имеет право расторгнуть субподряд и поручить субподрядчику аннулировать или вернуть персональные данные.

# Пункт 8 – Международные переводы

1. Согласованная в контракте обработка данных осуществляется исключительно на территории государства-члена Европейского Союза (ЕС) или государства-члена Европейской экономической зоны (ЕЭЗ).
2. Любая передача данных подрядчиком в третью страну или международную организацию должна осуществляться только на основании документированных инструкций GIZ или для выполнения конкретного требования в соответствии с законодательством Союза или государства-члена, которому подчиняется подрядчик, и должен принять место в соответствии с Главой V Регламента (ЕС) 2016/679.
3. GIZ соглашается, что если подрядчик привлекает субподрядчика в соответствии с Оговоркой 7 для выполнения конкретных действий по обработке (от имени GIZ) и эти действия по обработке включают передачу персональных данных в значении Главы V Регламента (ЕС) 2016/679, подрядчик и субподрядчик могут обеспечить соблюдение Главы V Регламента (ЕС) 2016/679 путем использования стандартных контрактных Оговорок, принятых Комиссией в соответствии со статьей 46(2) Регламента (ЕС) 2016/679, при соблюдении условий для использования этих стандартных контрактных Оговорок.

# Пункт 9 – Помощь GIZ

1. Подрядчик должен незамедлительно уведомить GIZ о любом запросе, полученном от субъекта данных. Он не должен отвечать на сам запрос, если только он не уполномочен на это GIZ.
2. Подрядчик должен помочь GIZ в выполнении ее обязательств по реагированию на запросы субъектов данных об осуществлении их прав, принимая во внимание характер обработки. При выполнении своих обязательств в соответствии с (a) и (b) подрядчик должен соблюдать инструкции GIZ.
3. В дополнение к обязательству подрядчика по оказанию помощи GIZ в соответствии с Оговоркой 9(b), подрядчик должен также оказывать помощь GIZ в обеспечении соблюдения следующих обязательств, принимая во внимание характер обработки данных и информацию, доступную подрядчику:
   1. обязательство провести оценку влияния предусмотренных операций по обработке на защиту персональных данных («оценка воздействия на защиту данных»), если тип обработки может привести к высокому риску для прав и свобод физических лица;
   2. обязательство проконсультироваться с компетентным надзорным органом перед обработкой, если оценка воздействия на защиту данных показывает, что обработка приведет к высокому риску в отсутствие мер, принятых GIZ для снижения риска;
   3. обязательство обеспечивать точность и актуальность персональных данных, незамедлительно информируя GIZ, если подрядчику становится известно, что персональные данные, которые он обрабатывает, являются неточными или устарели;
   4. обязательства, предусмотренные статьей 32 Регламента (ЕС) 2016/679.
4. Стороны должны указать в Приложении III соответствующие технические и организационные меры, с помощью которых подрядчик должен оказать помощь GIZ в применении настоящей Оговорки, а также объем и степень требуемой помощи.

# Пункт 10. Уведомление об утечке персональных данных

В случае утечки персональных данных Подрядчик должен сотрудничать с GIZ и оказывать ей содействие в выполнении ее обязательств в соответствии со статьями 33 и 34 Регламента (ЕС) 2016/679, где это применимо, с учетом характера обработки и имеющейся у Подрядчика информации.

# Утечка данных, касающихся данных, обрабатываемых GIZ

В случае утечки персональных данных, касающихся данных, обрабатываемых GIZ, подрядчик должен помочь GIZ:

1. уведомив об утечке персональных данных компетентный надзорный орган без неоправданной задержки после того, как об этом стало известно GIZ, где это уместно (за исключением случаев, когда утечка персональных данных маловероятно приведет к риску для прав и свобод физических лиц);
2. при получении следующей информации, которая в соответствии со статьей 33(3) Регламента (ЕС) 2016/679 должна быть указана в уведомлении GIZ и должна как минимум включать:
   1. характер персональных данных, включая, где это возможно, категории и приблизительное количество соответствующих субъектов данных, а также категории и приблизительное количество соответствующих записей персональных данных;
   2. вероятные последствия утечки персональных данных;
   3. меры, принятые или предлагаемые к принятию GIZ для устранения утечки персональных данных, включая, при необходимости, меры по смягчению возможных негативных последствий.

Если и поскольку невозможно предоставить всю эту информацию одновременно, первоначальное уведомление должно содержать имеющуюся на тот момент информацию, а дополнительная информация, по мере ее поступления, должна предоставляться впоследствии без неоправданной задержки.

1. в соблюдении в соответствии со статьей 34 Регламента (ЕС) 2016/679 обязательства без неоправданной задержки сообщать субъекту данных о нарушении персональных данных, когда нарушение персональных данных может привести к высокому риску для прав и свобод физических лиц.

# Утечка данных, касающихся данных, обрабатываемых подрядчиком

В случае утечки персональных данных, касающихся данных, обработанных подрядчиком, подрядчик должен уведомить GIZ без неоправданной задержки после того, как подрядчику стало известно о нарушении. Такое уведомление должно содержать, как минимум:

1. описание характера нарушения (включая, если возможно, категории и приблизительное количество субъектов данных и соответствующих записей данных);
2. сведения контрактного пункта, где можно получить дополнительную информацию об утечке персональных данных;
3. его вероятные последствия и меры, принятые или предлагаемые к принятию для устранения нарушения, в том числе для смягчения его возможных неблагоприятных последствий.

Если и поскольку невозможно предоставить всю эту информацию одновременно, первоначальное уведомление должно содержать имеющуюся на тот момент информацию, а дополнительная информация, по мере ее поступления, должна предоставляться впоследствии без неоправданной задержки.

Стороны должны указать в Приложении III все другие элементы, которые должны быть предоставлены подрядчиком при оказании помощи GIZ в соблюдении обязательств GIZ согласно Статьям 33 и 34 Регламента (ЕС) 2016/679.

# Пункт 11. Несоблюдение Оговорок и прекращение действия.

1. Без ущерба для каких-либо положений Регламента (ЕС) 2016/679 в случае, если подрядчик нарушает свои обязательства по настоящим Оговоркам, GIZ может поручить подрядчику приостановить обработку персональных данных до тех пор, пока последний не выполнит требования настоящих Оговорок или контракт будет расторгнут. Подрядчик должен незамедлительно проинформировать GIZ, если он по какой-либо причине не сможет выполнить данные Оговорки.
2. GIZ имеет право расторгнуть контракт, если он касается обработки персональных данных в соответствии с настоящими Оговорками, если:
   1. обработка персональных данных подрядчиком была приостановлена ​​GIZ в соответствии с пунктом (а), и если соответствие настоящим Оговоркам не будет восстановлено в течение разумного периода времени и в любом случае в течение одного месяца после приостановки;
   2. подрядчик существенно или систематически нарушает настоящие Оговорки или свои обязательства в соответствии с Регламентом (ЕС) 2016/679;
   3. подрядчик не выполняет обязательное решение компетентного суда или компетентного надзорного органа относительно своих обязательств в соответствии с настоящими Оговорками или Регламентом (ЕС) 2016/679.

Если GIZ расторгает контракт по одной из вышеупомянутых причин, то такое расторжение считается ответственностью подрядчика в соответствии с разделом 5.3.2 Условий.

1. Подрядчик имеет право расторгнуть контракт, если он касается обработки персональных данных в соответствии с настоящими Оговорками, если после информирования GIZ о том, что ее инструкции нарушают применимые законодательные требования в соответствии с Оговоркой 6.1 (b), GIZ настаивает на соблюдении инструкций.
2. После прекращения действия контракта подрядчик должен вернуть все персональные данные, обработанные от имени GIZ, в GIZ и удалить существующие копии, если только законодательство Союза или государства-члена не требует хранения персональных данных. До тех пор, пока данные не будут удалены или возвращены, обработчик должен продолжать обеспечивать соблюдение настоящих Оговорок.
3. Носители данных и записи данных, предоставленные подрядчику, остаются собственностью GIZ.

# Приложение I. Описание обработки

Следующий выбор был сделан GIZ. Если подрядчик заметит пробелы, ошибки или неясности в контексте процедуры присуждения контракта или выполнения заказа, уведомление должно быть отправлено в GIZ.

Характер, цель и продолжительность обработки

* Предмет и срок аутсорсинга обработки данных, а также объем, характер и цель обработки персональных данных определяются Техническим заданием и предложением, представленным подрядчиком.
* Подробное описание объема, характера и цели обработки:

Категории субъектов данных, чьи персональные данные обрабатываются

* Сотрудники GIZ, включая заявителей
* Подписчики, например, журналов и информационных бюллетеней
* Внешние участники мероприятий
* Участники опросов
* Посетители в помещении GIZ
* Посетители веб-сайтов
* Поставщик услуг/Поставщик
* Контактные лица учреждений-партнеров
* Представители официальных органов и представители правительства
* Студенты/стипендиаты
* Другое:

Категории обрабатываемых персональных данных

* Персональные основные данные (имя, дата рождения)
* Адресные данные
* Контактные и коммуникационные данные (например, телефон, электронная почта и т. д.)
* Данные о квалификации (например, история карьеры, резюме, квалификация и т. д.)
* Данные о сотрудниках (заработная плата, банковский счет, налоговая информация и т. д.)
* Данные по выставлению счетов и платежные данные
* Пользовательские данные (данные просмотра, IP-адреса, файлы cookie, данные для входа и т. д.)
* Фото и звукозаписи
* Данные о поездках и местоположении
* Особые категории персональных данных в соответствии со статьей 9 Регламента (ЕС) 2016/679 (например, данные о здоровье, биометрические данные, данные, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения или данные, касающиеся сексуальной жизни физического лица, или сексуальная ориентация).
* Другое:

# Приложение II – Список субподрядчиков

* Подрядчик не может передавать субподрядчикам какие-либо операции по обработке, выполняемые от имени GIZ в соответствии с настоящими Оговорками.

GIZ соглашается на привлечение следующих субподрядчиков:

|  |  |  |  |
| --- | --- | --- | --- |
| ФИО | Адрес вкл. cтрану | Описание обработки (включая предмет, характер и продолжительность) | При передаче данных в третью страну или международную организацию: Как обеспечивается соблюдение Главы V Регламента  (ЕС) 2016/679? |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Приложение III – Технические и организационные меры (ТОМ), включая технические и организационные меры по обеспечению безопасности данных

Описание технических и организационных мер безопасности, реализуемых подрядчиком (включая любые соответствующие сертификаты) для обеспечения надлежащего уровня безопасности с учетом характера, объема, контекста и цели обработки, а также рисков для прав и свобод физических лиц.

Для презентации можно использовать следующий контрольный список, содержащий большое количество возможных технических и организационных мер. Контрольный список не является исчерпывающим и при необходимости должен дополняться подрядчиком для каждого отдельного случая. Чтобы обеспечить конкретное описание, в каждом случае должны быть вставлены пояснения.

Презентация и описание технических и организационных мер, реализованных подрядчиком, также могут быть оформлены в отдельном документе.

# Меры псевдонимизации и шифрования персональных данных

* + Псевдонимизация персональных данных в открытом виде больше не требуется.
  + Политика псевдонимизации
  + Шифрование носителей данных
  + Псевдонимизация данных тест-системы
  + Шифрование веб-сайтов (SSL)
  + Шифрование базы данных
  + Шифрование электронной почты (TLS 1.2 или 1.3)
  + Шифрование паролей и ключей
  + Шифрование мобильных устройств
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по обеспечению постоянной конфиденциальности, целостности, доступности и устойчивости систем обработки и услуг.

* + Соглашение о неразглашении с сотрудниками
  + Обязанности сотрудников по защите данных
  + Соглашение о неразглашении с третьими лицами
  + Внешнее хранилище/сервер резервного копирования
  + Сопровождение контрактов с третьими лицами
  + Соглашения о передаче данных на аутсорсинг
  + Использование сертифицированного облачного провайдера
  + Брандмауэр
  + Антивирусная программа
  + Регулярное резервное копирование данных
  + Резервированные системы
  + Мониторинг систем и сервисов
  + RAID-системы
  + Сетевое хранилище (NAS)
  + Контракт на техническое обслуживание
  + Регулярные тесты на ИТ-инциденты
  + Внутреннее хранилище копий/резервных копий
  + Источник бесперебойного питания (ИБП),
  + Системы пожарной и дымовой сигнализации
  + Устройства контроля температуры
  + Противопожарное оборудование
  + Предупреждение о несанкционированном доступе
  + Балансировка нагрузки
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по обеспечению возможности своевременного восстановления доступности и доступа к персональным данным в случае физического или технического инцидента.

* + Регулярное резервное копирование всей системы.
  + Хранение в нескольких системах
  + Концепция резервного копирования данных
  + Регулярное тестовое резервное копирование/восстановление
  + Соглашение о поддержке и обслуживании оборудования
  + Концепция готовности к чрезвычайным ситуациям
  + Резервное копирование данных аутсорсинга
  + Регулярное обучение ИТ-персонала
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Процессы регулярного тестирования, анализа и оценки эффективности технических и организационных мер для обеспечения безопасности обработки.

* + Система внутреннего контроля
  + Контроль заказов или контрактов (тщательный отбор подрядчиков, четкая структура контракта и т. д.)
  + Регулярный анализ ИТ-процессов
  + Регулярные проверки (например, со стороны специалиста по защите данных)
  + Регулярный пересмотр процедур
  + Аудит технических и организационных мер специалистом по защите данных
  + Регулярные проверки сотрудников
  + Проведение оценки воздействия защиты данных
  + Проверка конфиденциальности задумана и по умолчанию
  + Система управления защитой данных/руководство по защите данных
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по идентификации и авторизации пользователей

* + Двухфакторная авторизация
  + Авторизация по имени пользователя/паролю
  + Разделение ролей между тестовой и производственной системой
  + Регулярная оценка разрешений
  + Пароли BIOS
  + Управление разрешениями
  + Политика управления мобильными устройствами
  + Профили пользователей
  + Политика паролей
  + Ограничение количества администраторов
  + Идентификация новых сотрудников
  + Разделение ролей пользователей
  + Автоматические запирающие механизмы
  + Идентификация внешнего лица с помощью ID-карты
  + Управление правами администратором
  + Различие между разрешениями
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по защите данных при передаче

* + Использование технологий шифрования
  + Virtual Private Network (Виртуальная частная сеть) (VPN)
  + Протоколирование действий и событий
  + Транспорт через частное облако
  + Документирование получателей данных
  + Шифрование электронной почты (TLS 1.2 или 1.3)
  + Проверка личности получателей
  + Использование частных дисков
  + Физический транспорт: безопасные транспортные контейнеры
  + Тщательный подбор транспортного персонала
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по защите данных при хранении

* + Шифрование носителей данных
  + Классификация данных
  + Управление разрешениями
  + Ограничение доступа
  + Логирование действий и событий
  + Бронированные двери
  + Ограничение количества администраторов
  + Магнитные или чиповые карты
  + Анонимизация данных
  + Псевдонимизация данных
  + Безопасное хранение носителей информации
  + Брандмауэр
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по обеспечению физической безопасности мест обработки персональных данных

* + Система сигнализации
  + Службы безопасности объекта и/или сотрудники службы безопасности на входе
  + Защита шахт зданий
  + Регистрация посетителей
  + Автоматический контроль доступа
  + Тщательный подбор клинингового персонала.
  + Тщательный подбор сотрудников службы безопасности.
  + Магнитные или чиповые карты

☐ Система запирания с кодовым замком

☐ Обязанность носить карты авторизации

☐ Ручная система запирания

☐ Концепция доступа

☐ Биометрический входной барьер

☐ Запираемые серверные шкафы

☐ Видеонаблюдение на входе

☐ Двери с ручкой снаружи

☐ Световые барьеры/датчики движения

☐ Посетители: только в сопровождении сотрудников

☐ Предохранительные замки

☐ Система звонков с камерой

☐ Процедура выдачи ключей

* + ​

​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по обеспечению протоколирования событий

* + Использование автоматического протоколирования
  + Создание отчетов об инцидентах
  + Уведомление с тревогой в реальном времени
  + Ведение журнала на уровне приложения
  + Автоматический просмотр журналов
  + Синхронизация системных часов
  + Регулярная ручная проверка журналов
  + Автоматическая консолидация инцидентов
  + Журналы сохраняются в приложении и автоматически отправляются в другое место.
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по обеспечению конфигурации системы, включая конфигурацию по умолчанию

* + Существует политика управления конфигурацией.
  + Процесс внесения изменений в конфигурации
  + Конфиденциальность по умолчанию
  + Проверка конфигураций по умолчанию
  + Определение конфигураций по умолчанию
  + Конфигурация системным администратором
  + Логирование изменений в конфигурациях
  + Регулярное обучение ИТ-персонала
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по регулированию и управлению внутренними ИТ и ИТ-безопасностью

* + Руководство по ИТ-безопасности
  + Руководство по ИТ-администрированию
  + Регулярные проверки/обзоры соответствия
  + Реестр ИТ-систем
  + Обучение сотрудников вопросам безопасности данных
  + Регулярный обзор/оценка системы
  + ИТ-команда с назначенными ролями/обязанностями
  + Рекомендации по управлению инцидентами
  + Оценка рисков и меры по управлению рисками на всех этапах и уровнях
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по сертификации/гарантии процессов и продукции

* + Внедрение ISO 9001 – Менеджмент качества
  + Внедрение ISO 27001 – Система менеджмента информационных технологий.
  + Внедрение ISO 27701 – Система управления конфиденциальной информацией
  + GDPR-сертификация – управление защитой данных
  + Обзор правил, применимых к продуктам/услугам/процессам
  + Определение отраслевых стандартов
  + Регулярные внутренние и/или внешние аудиты
  + Возложение аудиторских обязанностей на сертифицированных экспертов
  + Регулярная проверка новых требований и продление сертификатов
  + ​

Объяснение: В Кыргызстане нет требований по ИТ-аудиту и сертификации в компании

# Меры по обеспечению минимизации данных

* + Определение цели обработки
  + Оценка связи между обработкой и целью
  + Оценка объема и качества обрабатываемых данных в соответствии с целью
  + Определение применимых периодов хранения
  + Безопасное удаление данных после истечения срока хранения.
  + ​

Объяснение:

# Меры по обеспечению качества данных

* + Профилирование и классификация данных
  + Контроль входящих или новых данных
  + Логирование ввода/изменения данных
  + Передача прав на ввод данных
  + Хранение журнала
  + Отслеживание пользователей при входе, изменение данных (без групп пользователей)
  + Избежание дублирования данных
  + Определение требований к данным
  + Применение мер качества данных
  + ​

Объяснение:

# Меры по обеспечению ограниченного хранения данных

* + Политика хранения с ролями
  + Разделение данных по срокам хранения
  + Регулярное обучение
  + Регулярный просмотр и оценка сохраненных данных
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по обеспечению подотчетности

* + Обучение/повышение осведомленности
  + Регулярные проверки и аудиты
  + Существует группа защиты данных
  + Руководство и поддержка сотрудников
  + Соответствующая политика конфиденциальности
  + Заключение стандартных контрактных Оговорок (SCC)
  + Соглашения о совместном контроле
  + Ответы на запросы субъектов данных
  + Документы о прозрачности (статья 13/14 GDPR)
  + Безопасное удаление данных
  + Документированное заявление о конфиденциальности
  + Аудиторские отчеты и меры документируются
  + Надлежащее участие Уполномоченного по защите данных
  + Особая процедура получения согласия/ведение журналов согласия
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |

# Меры по обеспечению переносимости данных и обеспечению их удаления

* + Хранение в структурированном формате
  + Мониторинг установленных законом сроков
  + Передача через сквозное шифрование
  + Соблюдение сроков хранения
  + Обеспечение переносимости данных
  + Рассмотрение прав субъектов данных в соответствии с главой 3 Регламента (ЕС) 2016/679.
  + Безопасное удаление данных гарантировано
  + Обеспечено безопасное уничтожение носителей информации
  + ​

|  |  |  |
| --- | --- | --- |
| Объяснение: |  |  |
|  | | |