Политика компании "АРЕНСИЯ" [ARENSIA] в сферах конфиденциальности и защиты данных

I. Политика защиты данных

В рамках своей деятельности компания "АРЕНСИЯ Експлоратори Медисин" [ARENSIA Exploratory Medicine] обеспечивает необходимое соответствие высокому уровню защиты персональных данных и требованиям многогранных положений Общего регламента ЕС о защите данных (GDPR). Эта политика касается всех сторон - работников, поставщиков, пациентов и спонсоров - которые оказывают нашей компании любые объемы информации.

Эта политика конфиденциальности данных применяется к компании "АРЕНСИЯ Експлоратори Медисин" [ARENSIA Exploratory Medicine] во всех странах мира и основывается на всемирно признанных фундаментальных принципах защиты данных. Для целей трансграничной передачи данных между подразделениями компаний эта политика содержит одно из необходимых рамочных условий, обеспечивая надлежащий уровень защиты данных, предусмотренный Общим регламентом ЕС о защите данных[1].

II. Применение национального законодательства

Общий регламент ЕС о защите данных применяется не только к организациям, расположенным в пределах ЕС, но и к организациям, расположенным за пределами ЕС, если они предлагают товары или услуги субъектам данных ЕС или осуществляют мониторинг их поведения. Он применяется ко всем компаниям - резидентам Европейского Союза, которые обрабатывают и содержат персональные данные субъектов данных, независимо от местонахождения компании.

III. Политика защиты данных - определение терминов

"Персональные данные" означает любую информацию, касающуюся физического лица, которая была идентифицирована или может быть идентифицирована; физическое лицо ("субъект данных"), которое может быть идентифицировано - это лицо, которое может быть идентифицировано, прямо или косвенно, в частности, на основе любого идентификатора, такого как фамилия, идентификационный номер, данные о местонахождении, Интернет-идентификатор, или на основе одного или нескольких факторов, присущих физической, физиологической, генетической, ментальной, культурной или социальной принадлежности такого физического лица;

"Обработка" означает любую операцию или совокупность операций, таких как сбор, регистрация, организация, структурирование, хранение, адаптирование, изменение, получение, консультация, использование, раскрытие путем передачи, распространения или предоставления другим образом, выверки или объединения, ограничения, удаление или уничтожение персональных данных или групп персональных данных, в том числе с использованием автоматизированных систем;

" *Контроллер* " означает физическое или юридическое лицо, государственный орган, агентство или другой орган, который самостоятельно или совместно с другими сторонами определяет цели и средства обработки персональных данных; если цели и средства такой обработки определяются законодательством Союза или государства-члена, законодательством Европейского Союза или государства-члена может быть назначен контроллер или определены конкретные критерии для его назначения;

"Обработчик» означает физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные от имени контроллера;

"*Получатель*" означает физическое или юридическое лицо, государственный орган, агентство или иной орган, которому раскрываются персональные данные, независимо от того, является или не является он третьей стороной. Однако органы государственной власти, которые могут получать персональные данные в рамках конкретного расследования в соответствии с законодательством Союза или государств-членов, не считаются получателями; обработка этих данных этими государственными органами должна соответствовать действующим правилам защиты данных в соответствии с целями обработки;

"Третья сторона» означает физическое или юридическое лицо, государственный орган, учреждение или орган, кроме субъекта данных, контроллера, обработчика и лиц, которые, согласно полномочиям, предоставленным непосредственно контроллером или обработчиком, имеют право обрабатывать персональные данные;

"Согласие» субъекта данных означает любое добровольно предоставленное, конкретное, информированное и однозначное сообщение о желании субъекта данных, с помощью которого он или она заявлением или однозначным положительным действием выражает согласие на обработку персональной информации, касающейся его или ее ;

"Трансграничное обработка" - обработка персональных данных, которая происходит в контексте деятельности одного учреждения контроллера или обработчика в Союзе, однако которая существенно влияет или может влиять на субъектов данных в более чем одном государстве-члене.

"Должностное лицо по вопросам защиты данных» - лицо, назначенное контроллером и обработчиком персональных данных для выполнения задач и обязанностей, определенных Союзом. Он / она не получает никаких указаний по выполнению им / ею задач, не может быть наказан(а) за выполнение своих задач, подчиняется непосредственно высшему руководству и обязан(а) хранить тайну или конфиденциальность в отношении выполнения своих задач. Задачи Должностного лица по вопросам защиты данных определены в разделе XII .

IV. Принципы обработки персональных данных

1. Законность, честность и прозрачность

Персональные данные должны обрабатываться законно, справедливо и прозрачно по отношению к субъекту данных.

2. Ограничение целей

Персональные данные должны собираться для конкретных, явных и законных целей и не обрабатываться в дальнейшем способом, несовместимым с этими целями; дальнейшая обработка для целей архивирования в общественных интересах, для целей научных или исторических исследований или статистических целей, в соответствии со статьей 89 (1)[2], не может считаться несовместимой с первоначальными целями.

3. Минимизация и точность данных

Собранные персональные данные должны быть адекватными, существенными и ограниченными тем, что необходимо для достижения целей, для которых они обрабатываются. Данные должны быть точными и, при необходимости, актуализированными; необходимо принять все разумные шаги для того, чтобы персональные данные, которые

являются неточными, учитывая цели, для которых они обрабатываются, были немедленно удалены или исправлены.

4. Ограничение на хранение

Персональные данные должны храниться в форме, которая позволяет идентифицировать субъектов данных не дольше, чем это необходимо для целей, для которых обрабатываются персональные данные; персональные данные могут храниться в течение более длительных периодов, если персональные данные будут обрабатываться исключительно для архивирования в интересах общества, для целей научных или исторических исследований или статистических целей в соответствии со статьей 89 (1)[3] при условии применения соответствующих технических и организационных мероприятий, требуемых настоящим регламентом для обеспечения защиты прав и свобод субъекта данных.

5. Целостность и конфиденциальность

Собранные данные должны обрабатываться таким образом, чтобы обеспечить надлежащий уровень безопасности персональных данных, включая защиту от несанкционированной или незаконной обработки и случайной потери, уничтожения или повреждения, с использованием соответствующих технических или организационных средств.

V. Надежность обработки данных

Сбор, обработка и использование персональных данных разрешаются только с учетом изложенных ниже правовых основ Общего регламента ЕС о защите данных. Конфиденциальность и безопасность собранных персональных данных является приоритетом для "АРЕНСИЯ Експлоратори Медисин" [ARENSIA Exploratory Medicine], и для компании "АРЕНСИЯ" не менее важным является обеспечение понимания всеми того, как мы обрабатываем эти данные:

1. Данные пациентов

Для проведения клинического испытания в соответствии с положениями Хельсинкской декларации и Международного комитета по гармонизации (ICH) в отношении надлежащей клинической практики (GCP) мы собираем данные в объеме, описанном в одобренном и утвержденном голосованием протоколе испытаний. Такие данные могут включать информацию, касающуюся состояния здоровья, и другую конфиденциальную информацию.

2. Данные сотрудников

Для ведения бизнеса в глобальном масштабе и выполнения требований государственных нормативных актов (о трудоустройстве, налогообложении, страховании и т.п.) мы собираем различные персональные и другие данные в зависимости от ваших трудовых обязанностей, гражданства, места работы и других факторов.

Такие данные могут включать:

- Имя, фамилию;
- Идентификационный номер;
- Номер телефона,
- Адрес эл. почты
- Банковские и другие финансовые данные;

- Государственные идентификационные номера, в т.ч. номера социального страхования, идентификационные данные налогоплательщика, номер водительского удостоверения;
- Данные о семье.

Мы можем использовать данные следующим образом:

- для идентификации определенного лица;
- для целей обмена данными с любым лицом;
- для удовлетворения потребностей в человеческих ресурсах;
- для выполнения правительственных предписаний и постановлений;
- для осуществления выплат работникам (компенсации, медицинское страхование, возмещение расходов и т.п.).

3. Данные клиентов и третьих сторон

Для ведения бизнеса и выполнения договорных обязательств мы собираем данные партнеров по договорам, таких как спонсоры, субподрядчики и поставщики. Такие данные могут включать название, адрес электронной почты компании, номер телефона компании, банковские и другие финансовые реквизиты и данные компании. Компания "АРЕНСИЯ" принимает меры с целью обеспечить предоставление третьим сторонам только персональных данных, определенных инструкциями, и ограничить такое предоставление раскрытием данных агентам и субподрядчикам поставщика при условии получения компанией "АРЕНСИЯ" предварительного письменного согласия клиента или третьей стороны, или обеспечить предоставление данных в случаях, когда соответствующее раскрытие информации требуется законом.

VI. Обработка данных контрактов

Обработка данных от имени кого-то означает, что провайдер привлекается для обработки персональных данных, но не несет при этом ответственности за соответствующий бизнес-процесс. В этих случаях с внешними провайдерами и аффилированными компаниями в составе "АРЕНСИЯ" должно быть заключено соглашение о защите данных от имени. Клиент несет полную ответственность за правильное выполнение обработки данных. Провайдер может обрабатывать персональные данные только в соответствии с инструкциями клиента. Такие услуги могут использоваться для целей учета заработной платы на местах.

VII. Права субъекта данных

1. Право доступа

Частью расширенных прав субъектов данных, указанных в Общем регламенте ЕС о защите данных, является право субъектов данных получать от контроллера данных подтверждение того, обрабатываются ли их персональные данные, где и с какой целью они обрабатываются. Кроме того, контроллер обязан бесплатно предоставить копию персональных данных в электронном формате. Это изменение является резким переходом к обеспечению прозрачности данных и расширения возможностей субъектов данных.

2. Право на исправление

Субъект данных имеет право без лишней задержки получить от контроллера исправления неточных персональных данных, касающихся его или ее. Принимая во внимание цели обработки, субъект данных имеет право требовать дополнения неполных персональных данных, в том числе путем подачи дополнительного заявления.

3. Право на забвение

Известное также, как Стирание данных, право на забвение дает право субъекту данных требовать от контроллера данных удаления его / ее персональных данных, прекращение дальнейшего распространения данных и потенциального прекращения обработки данных третьими лицами. Условия удаления включают данные, которые более не являются существенными для определяющих целей обработки или отзыва согласия субъектами данных. Следует также отметить, что это право требует от контроллеров сравнивать права субъектов с "общественным интересом в наличии данных" в процессе рассмотрения таких запросов.

4. Право на ограничение обработки

Условия получения согласия ужесточаются, поскольку запрос на согласие подается в понятной и легкодоступной форме, при этом к согласию добавляется информация о цели обработки данных. Согласие является четкой и отличной от других вопросов и предоставляется в понятной и легкодоступной форме, используя четкую и понятную речь в каждом документе, предоставленном компанией "АРЕНСИЯ": трудовые договоры, договоры с клиентами и поставщиками, включая документы, предоставленные Спонсорами через компанию "АРЕНСИЯ", то есть Форма предоставления информированного согласия. Отозвать согласие так же легко, как и предоставить его.

5. Право на перенос данных

Общий регламент ЕС о защите данных создает возможность переноса данных - право субъектов данных получать персональные данные о них, которые они ранее предоставляли в "общепринятом и пригодном для машинного считывания формате", и имеют право передавать эти данные другому контроллеру.

6. Право на возражения

Субъект данных имеет право в любое время подавать возражения по основаниям, касающиеся его или ее конкретной ситуации, против обработки персональных данных, касающихся его или ее, согласно этим положениям. Контроллер теряет право обрабатывать персональные данные, если контроллер не продемонстрирует убедительные законные основания для обработки, которые преобладают над интересами, правами и свободами субъекта данных, или для установления, осуществления или защиты законных требований.

VIII. Конфиденциальность обработки

На персональные данные распространяются требования о секретности данных. Любой несанкционированный сбор, обработка или использование таких данных работниками запрещены. Любая обработка данных, осуществленная работником, на которую он / она не был уполномочен(а) в рамках своих законных обязанностей, является несанкционированной. При этом применяется принцип служебной необходимости. Работники могут иметь доступ к персональной информации только в случае, когда такой доступ согласуется с типом соответствующего задания. Это требует тщательного распределения, разграничения, а также реализации ролей и обязанностей.

Сотрудникам запрещено использовать персональные данные для частных или коммерческих целей, раскрывать их третьим лицам или предоставить их любым другим способом. Надзорные органы обязаны сообщать своим работникам в начале трудовых отношений об обязанности хранить секретность данных. Эта обязанность остается в силе даже после окончания трудовой деятельности.

IX. Безопасность обработки

Персональные данные должны быть защищены от несанкционированного доступа и незаконной обработки или раскрытия, а также от случайной потери, изменения или уничтожения. Это положение применяется независимо от того, в каком - электронном или бумажном - виде осуществляется обработка данных. До внедрения новых методов обработки данных, в частности, новых ИТ-систем, необходимо определить и реализовать технические и организационные меры по защите персональных данных. Эти меры должны осуществляться с применением самых современных средств и с учетом рисков обработки и необходимости защиты данных.

В частности, ответственный отдел может проконсультироваться с представителем департамента ИТ и Должностным лицом по вопросам защиты данных. Технические и организационные меры по защите персональных данных являются частью обязанностей Должностного лица по вопросам защиты данных и должны постоянно корректироваться с учетом технических достижений и организационных изменений.

X. Контроль защиты данных

Соответствие Политике защиты данных и действующему законодательству о защите данных регулярно проверяется путем проведения аудиторских проверок по вопросам защиты данных и применения других средств контроля. Использование этих средств контроля входит в обязанности Должностного лица по вопросам защиты и других подразделений компании, имеющих права на аудит, или привлеченных внешних аудиторов. О результатах контроля защиты данных необходимо уведомлять Должностное лицо по вопросам защиты данных. Управленческий персонал компании "АРЕНСИЯ Експлоратори Медисин" [ARENSIA Exploratory Medicine] должен быть проинформирован об основных результатах путем получения соответствующей отчетности. По запросу, результаты контроля защиты данных будут предоставлены органу, ответственному за защиту данных. Ответственный орган по вопросам защиты данных может осуществлять собственный контроль за соблюдением положений настоящей Политики в объеме, разрешенном национальным законодательством.

XI. Нарушение безопасности данных, ответственность и санкции

Предложенные положения об утечках данных, прежде всего, касаются нарушений положений корпоративной политики обмена сообщениями. Информация об утечках данных, приводящих к возникновению риска для физических лиц (например, несанкционированное раскрытие номера банковского счета или информации о медицинском страховании), должна предоставляться соответствующему Агентству по защите данных в течение 72 часов и пострадавшим лицам без лишней задержки.

XII. Должностное лицо по вопросам защиты данных

Должностное лицо по вопросам защиты данных выполняет роль лидера в сфере безопасности предприятия, как предусмотрено Общим регламентом ЕС о защите данных. Должностные лица по вопросам защиты данных несут ответственность за надзор за стратегией защиты данных и ее реализацией для обеспечения соответствия требованиям Общего регламента ЕС о защите данных.

Обязанности должностного лица по вопросам защиты данных:

- Обучение компании и сотрудников важным требованиям соответствия законодательству
- Обучение персонала, выполняющего обработку данных

- Проведение аудита для обеспечения соответствия и упреждающего решения потенциальных проблем

- Выполнение функций звена связи между компанией и надзорными органами, созданными в соответствии с положениями Общего регламента ЕС о защите данных

- Мониторинг эффективности и предоставление информации о результатах деятельности в сфере обеспечения защиты данных

- Ведение комплексного учета всех мероприятий по обработке данных, проводимых компанией, включая данные о цели всех видов обработки данных, которые должны быть обнародованы по запросу

- Взаимодействие с субъектами данных с целью проинформировать их о том, как используются их данные, об их правах на удаление их персональных данных и о том, какие меры компания приняла для защиты их персональной информации.

XIII. Защита данных в компании "АРЕНСИЯ"

Принципы, описанные в этой политике и предусмотренные требованиями Общего регламента ЕС о защите данных, реализуются в системах компании "АРЕНСИЯ" путем утверждения соответствующих Рабочих инструкций, охватывающих упомянутые темы.