EUROLAB “Cook Book” – Doc No. 22
Translated into Russian by LLC “Profilab” (with the permission of EUROLAB)

“Поваренная книга” EUROLAB – Документ No. 22
Переведено на русский язык ООО “Профилаб” (с разрешения EUROLAB)

GDPR – ОБЩИЙ РЕГЛАМЕНТ О ЗАЩИТЕ ДАННЫХ

Начиная с мая 2018 года новый Регламент ЕС 2016/679 (GDPR — Общий регламент по защите данных) о защите персональных данных вводит новые правила и требования к управлению данными, относящимися к физическим лицам. Эти новые требования также применимы к испытательным лабораториям, причем не только в отношении уже управляемых для целей сбора или учета персональных данных сотрудников, поставщиков и заказчиков, но и в отношении более рабочих аспектов, касающихся «технической регистрации», которую выполняют испытательные лаборатории.

Практическим примером этого утверждения является глава 7.5.1 стандарта ISO/IEC 17025:2017:

ISO/IEC 17025:2017 - § 7.5.1 «Лаборатория должна обеспечивать наличие в технических записях для каждого вида лабораторной деятельности результатов, отчета и достаточной информации, позволяющей, если это возможно, идентифицировать факторы, влияющие на результат измерения и связанную с ним неопределенность измерений, а также обеспечить возможность повторного проведения данной лабораторной деятельности в условиях, максимально близких к первоначальным. Технические записи должны включать дату и сведения о персонале лаборатории, который несет ответственность за каждый вид лабораторной деятельности и за проверку данных и результатов. Первичные наблюдения, данные и расчеты должны быть записаны в момент, когда они были получены, и должны отождествляться с конкретной работой».

Еще более важными являются так называемые «конфиденциальные» персональные данные, в соответствии с положениями статьи 9 GDPR «Обработка особых категорий персональных данных», которыми могут управлять лаборатории для некоторых видов технической квалификации персонала (например, квалификация персонала, занимающегося неразрушающими испытаниями или деятельностью в секторе медицинского обслуживания).

Поэтому лаборатории должны ознакомиться с терминологией, введенной GDPR, и установить соответствующие процедуры, чтобы гарантировать управление персональными данными наравне с тем, что было сделано до сих пор для технических данных.

Некоторые термины GDPR

Рекомендуя полностью прочитать статью 4 GDPR «Определения», мы приводим ниже некоторые ключевые слова, которые должны знать лаборатории и которые помогут нам понять значение нижеприведенного текста:

Выдержка из статьи 4 GDPR «Определения»

(1) «персональные данные» означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на такой идентификатор, как имя, идентификационный номер, данные о местоположении, сетевой идентификатор или на один или несколько факторов, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица;

(2) «обработка» означает любую операцию или набор операций, которые выполняются с персональными данными или с наборами персональных данных с применением или без применения автоматических средств, такие как сбор, запись, систематизация, структурирование,

хранение, адаптация или изменение, поиск, консультирование, использование, разглашение путем передачи, распространения или предоставления доступа иным способом, группирование или объединение, ограничение, стирание или уничтожение;

…

(7) «контролер» означает физическое или юридическое лицо, орган государственной власти, агентство или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных; если цели и средства такой обработки определяются законодательством Союза или государства-участника, контролер или специальные критерии его назначения могут быть предусмотрены законодательством Союза или государства-участника;

(8) «обработчик» означает физическое или юридическое лицо, орган государственной власти, агентство или другой орган, который обрабатывает персональные данные от имени контролера;

…

(11) «согласие» субъекта данных означает любое свободно данное, конкретное, осведомленное и недвусмысленное указание на пожелания субъекта данных, которым он или она путем заявления или четкого утверждения выражает согласие на обработку персональных данных, относящиеся к нему или к ней;

(12) «утечка персональных данных» означает нарушение безопасности, ведущее к случайному или незаконному уничтожению, потере, изменению, несанкционированному разглашению или доступу к передаваемым, хранимым или иным образом обрабатываемым персональным данным;

…

Основной фокус

GDPR устанавливает ряд правил, которые обязательно должны быть адаптированы к индивидуальным потребностям компании, которая должна их выполнять. Не существует такой вещи, как линия поведения, подходящая для всех реальностей. Однако существует два основных момента, которым должны следовать все, включая лаборатории:

- информация: GDPR уделяет большое внимание понятию информации, которую контролер должен предоставить субъекту данных. Также во многих случаях необходимо получить от субъекта данных явное «согласие» на использование персональных данных для конкретных целей, на которые они собираются.

- защита данных: после сбора данных важно защитить их таким образом, чтобы возможность несанкционированного использования, потери или кражи данных была сведена к минимуму.

Давайте ниже подробно рассмотрим, как выполнить на практике упомянутые выше два момента.

Информация

Вкратце, GDPR устанавливает, что персональные данные должны обрабатываться для конкретной цели и в течение определенного периода времени. Таким образом, вышеупомянутая основная информация (цель и продолжительность обработки) должна быть указана в письменном документе, который называется «уведомление о конфиденциальности».

В зависимости от типа запрашиваемых данных может потребоваться получение согласия субъекта данных.

Конечно цели сбора данных могут быть разнообразными: рабочие контракты, коммерческие контракты, маркетинг, информационные бюллетени, отправка документации. Таким образом, в том же уведомлении о конфиденциальности можно составить список целей, для которых субъект данных может предоставить свое согласие или не дать его.

Точно так же период обработки может иметь разную продолжительность или определяться в результате других событий, например: до завершения деятельности, период времени после завершения действия контракта, ...

Уведомление и согласие могут стать известны/быть собраны любыми средствами (бумага, интернет, почта, автоматические системы и т. д.) при условии, что субъект данных, давший согласие, и дата/время выдачи согласия четко идентифицируемы.

Все согласия должны быть доступны для национального органа по защите конфиденциальности.

Защита данных

Защита данных проходит через различные темы и разные рабочие режимы, которые непросты для понимания тем, кто не знаком с ИТ-системами.

Возможное решение для проведения анализа проблемы, выявления любых пробелов в ИТ-системах и перехода к их безопасности может заключаться в тщательном анализе рисков и последующей подготовке процедуры аварийного восстановления.

Ниже давайте приведем некоторые ключевые моменты для рассмотрения при анализе рисков.

Конфиденциальность данных

Обрабатываемые персональные данные должны храниться таким образом, чтобы свести к минимуму риски несанкционированного доступа, уничтожения или потери за счет соответствующих мер безопасности, т. е. за счет всех технических и организационных мер, которые лаборатория может применить на практике, чтобы гарантировать защиту, неприкосновенность частной жизни и конфиденциальность.

Если Контролер решит использовать электронные устройства или компьютерные программы для управления данными, должен быть обеспечен контролируемый доступ через уровни авторизации и гарантировано, что никакая обработка не противоречит закону или не отличается от той, для которой были собраны данные.

В особенности, Контролер должен принять определенные критерии и процедуры, предусмотренные статьей 33 GDPR, такие как использование идентифицирующего имени пользователя и пароля для доступа к данным, использование антивирусного программного обеспечения и периодического резервного копирования данных.

Меры безопасности

Обработка персональных данных электронными средствами допускается только при соблюдении определенных минимальных мер, среди которых выделяют:

- ✓ аутентификация компьютера;
- ✓ внедрение процедур управления учетными данными для аутентификации;
- ✓ применение системы авторизации;
- ✓ защита электронных средств и данных от незаконной обработки данных и несанкционированного доступа;
- ✓ внедрение процедур хранения надежных копий;
- ✓ внедрение методов шифрования или идентификационных кодов для обработки определенных данных, которые подходят для раскрытия информации организаций здравоохранения о здоровье или сексуальной жизни.

Для «уязвимых» (конфиденциальных) и судебных данных планируются добавочные меры в дополнение к тому, что уже было упомянуто как Документ о политике безопасности.

Статья 34 GDPR четко предусматривает, что внедряются процедуры для создания и хранения резервных копий и восстановления доступа к данным и системам. На практике Контролер через

системного администратора ИТ должен обеспечить создание и хранение резервных копий системы или резервных копий данных и информации, содержащихся на отдельных электронных устройствах.

Причина потери данных и информации может зависеть от:

- ✓ разрушительных событий, природных или искусственных;
- ✓ отказов системы;
- ✓ неисправностей или разрушений электронных компонентов;
- ✓ невнимательности и халатности.

Риск потери данных может быть представлен через:

- ✓ недобросовестное поведение и обман;
- ✓ компьютерные вирусы;
- ✓ кражу мобильных устройств, содержащих данные.

В таких ситуациях резервное копирование может ограничить потерю хранимой информации. Однако и в этом случае данные, введенные в резервные копии, должны сохраняться и защищаться от нежелательного доступа с помощью процедур, препятствующих считыванию содержащихся в них данных, возможно, с использованием криптографического приложения.

Если используется сервер хранения данных, он должен быть подключен к источнику бесперебойного питания, чтобы не допустить потерю данных из-за колебаний напряжения или прекращения подачи энергии.

В случае потери данных необходимо незамедлительно применить все возможные процедуры восстановления данных.

Цифровая подпись

Цифровая подпись позволяет обмениваться цифровыми документами, имеющими юридическую силу, поскольку позволяет проверить личность отправителя, делает невозможным для отправителя пренебрегать подписанным документом, делает невозможным для получателя вносить изменения в документ, подписанный кем-то другим.

С технической точки зрения цифровая подпись представляет собой последовательность байтов, способную однозначно связать электронный документ с лицом, его создавшим, гарантируя его происхождение, подлинность и целостность.

Безопасность системы

Закон предусматривает, что обработка персональных данных с помощью электронных средств разрешена лицам, прошедшим обучение и получившим специальные профили авторизации, с целью ограничения доступа к данным, которые необходимы строго для выполнения заданных операций по обработке. Периодически, и в любом случае ежегодно, необходимо проверять наличие условий сохранения профилей авторизации.

Персональные данные также должны быть защищены от риска внешнего вторжения и от действия программ, которые могут нарушить конфиденциальность. По этой причине необходимо настроить подходящие электронные инструменты для предотвращения уязвимости систем и исправления любых неисправностей, такие как антивирус, антишпионское ПО и брандмауэры, которые должны обновляться не реже одного раза в шесть месяцев.

Не реже одного раза в год необходимо обновлять системы для исправления ошибок. Эту операцию легко можно выполнить также путем загрузки из Интернета патчей или пакетов обновлений, т.е. новых версий операционных систем и различных прикладных программ.

Управление паролями

Стороны, которым разрешен доступ к системам, могут сделать это, если у них есть учетные данные для аутентификации, состоящие из кода, связанного с ответственным лицом, и конфиденциального и секретного ключевого слова, известного только ответственному лицу, или с использованием персональных смарт-карт. Код, связанный с новым участником, или идентификатор пользователя, или имя пользователя, однажды использованные, не могут быть присвоены другим субъектам даже в другое время.

Сотрудники должны быть осведомлены о необходимых мерах предосторожности для обеспечения секретности ключевого слова и прилежном хранении устройств, находящихся исключительно в пользовании ответственного лица, а также не оставлять электронный инструмент без присмотра и общедоступным во время сеанса обработки (для этой цели системы позволяют установить экранную заставку с запросом пароля).

Хорошей идеей является деактивация неиспользуемых учетных данных для аутентификации по истечении определенного периода времени (например, 6 месяцев).

Защита бумажных архивов

Особое значение придается бумажным архивам, особенно в тех случаях, когда в них содержатся конфиденциальные данные, касающиеся сотрудников, информация о дисциплинарных разбирательствах, судебные данные, касающиеся тендеров, или информация, касающаяся коммерческих сделок, таких как счета-фактуры или контракты.

Контролерам должны быть даны конкретные письменные инструкции, которые предусматривают хранение документов. Доступ к архивам, содержащим конфиденциальные или судебные данные, должен быть разрешен только персоналу, который был специально обучен и уполномочен, и должен контролироваться. Поэтому необходимо принять политику, направленную на управление бумажными данными, содержащимися в архивах. В этом случае необходимо проверить доступ ранее авторизованных работников в помещения, где хранятся такие базы данных. Такую операцию можно выполнить, установив считыватель бейджей, который позволяет распознавать авторизованный субъект и разрешает доступ.

Окончание обработки

Важно определить методы управления персональными данными по окончании периода обработки.

Принимая во внимание тип обрабатываемых данных, для разных целей может потребоваться установить разные методы, в том числе относящиеся к одному и тому же субъекту данных; давайте рассмотрим несколько примеров:

при увольнении работника некоторые типы персональных данных (адрес электронной почты компании, доступ к информационным системам, контакты членов семьи для непредвиденных случаев и т. д.) могут быть немедленно аннулированы или может быть обеспечена их анонимность, в то время как другие типы данных могут быть удалены или сделаны анонимными в течение определенного периода времени (домашний адрес, личный номер телефона, ...), а некоторые другие данные, такие как имя и фамилия и данные, относящиеся к технической квалификации персонала, подписавшего протокол испытаний, должны сохраняться в течение очень длительного периода времени (10 лет и более).

В любом случае по истечении сроков, установленных действующим законодательством и содержащихся в уведомлении о конфиденциальности, персональные данные должны стать недоступными для обработки и ознакомления. Поэтому информацию, содержащуюся в базах данных и в средствах обеспечения для создания резервных копий (резервное копирование или другие средства аварийного восстановления), также придется стирать или делать анонимными.

За перевод настоящей CookBook и любые дополнительные правки несет ответственность ООО «Профилаб».