Data Privacy Office

ЧТО ТАКОЕ

GDPR

Data
Privacy
Office

Содержание

Немного предыстории...

С появлением и развитием технологий люди стали более щедрыми на персональные данные, ведь взамен они получают удобство и комфорт. Мы настолько привыкли к этому, что не можем представить наш мир иначе. Однако означает ли это, что жить теперь безопаснее? Отнюдь. Вся эта информация вполне может быть использована против нас самих. И мы, субъекты данных, потеряли контроль над своими персональными данными в новой цифровой реальности.

Европейцы всерьез занялись этим вопросом. Как результат, 27 апреля 2016 года приняли Общий Регламент защиты персональных данных (General Data Protection Regulation). Начал применяться новый закон только спустя два года (25 мая 2018 года), чтобы у бизнеса был запас времени к нему подготовиться. Правила GDPR значительно дополнили прежние нормы защиты приватности в Европе, которым было практически два десятилетия. Это вызвало множество вопросов у бизнеса: что делать? к кому обращаться? насколько опасно несоблюдение требований?

Авторы:

Дата Прайваси Офис - международная тренинговая и консалтинговая компания в сфере защиты персональных данных. Приводим ИТ-продукты компаний в соответствие с мировыми стандартами по приватности.

Data Privacy Office

Что такое GDPR?

Вы когда-нибудь задумывались, где хранятся отпечатки пальцев или снимки лица для разблокировки смартфона? Или для чего при оформлении заказа в интернет-магазине вас просят указать дату рождения, что, казалось бы, лишняя информация для покупки? Может ли кто-то получить доступ к вашей медицинской карте в поликлинике? Как организации находят ваш номер телефона, чтобы позвонить и рассказать о выставке или акции? Или что знают социальные сети о своих пользователях?

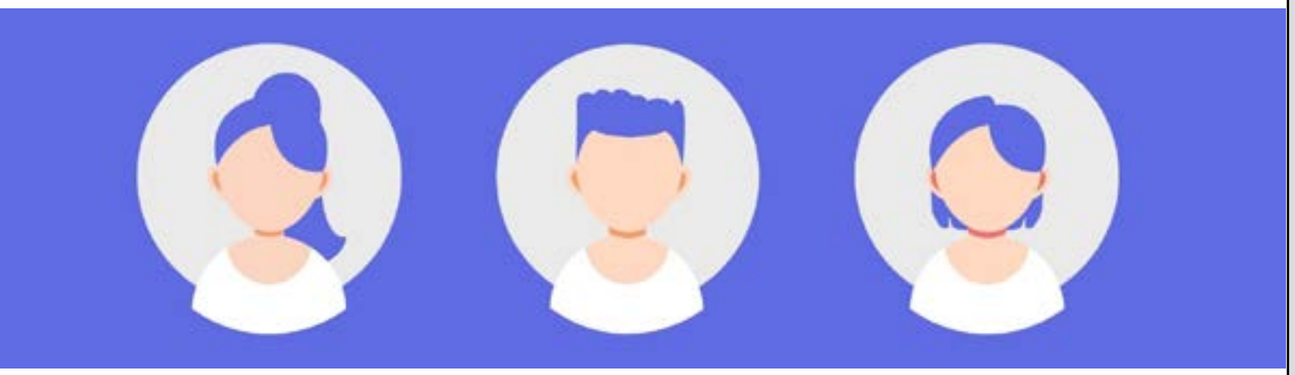
Каждый день мы делимся с окружающими тем, что принято называть персональными данными. Например, во время знакомства или общения, при поиске работы или записи на прием к доктору, заказывая товары, оплачивая услуги. При этом даже не задумываясь, что будет происходить с этими данными дальше.

27 апреля 2016 года

27 апреля 2016 года был принят Общий Регламент защиты персональных данных (GDPR). Начал применяться новый закон только спустя два года (25 мая 2018 года), чтобы у бизнеса был запас времени к нему подготовиться.

Что такое персональные данные?

Во всех вопросах, которые касаются действия Регламента, важную роль играет понятие персональных данных, ведь GDPR защищает именно персональные (а не анонимные) данные. Разберемся в определении более подробно.



Персональные данные

это любая информация, которая относится к идентифицированному или поддающемуся идентификации физическому лицу («субъекту данных», т. е. к человеку).

Идентифицированное физическое лицо

это человек, идентификатор (имя, номер телефона, личный номер, логин и т. д.) которого имеется среди данных.

Поддающееся идентификации физическое лицо

это лицо, которое вполне можно идентифицировать, то есть отличить от других людей.

Персональными данными является не только сам идентификатор, но и относящаяся к человеку информация. И здесь существуют свои нюансы.

Имя, номер паспорта, ID удостоверения, логин, никнейм, адрес электронной почты, номер телефона, IP-адрес, данные банковских карт – всегда персональные данные, потому что являются идентификаторами.

Номер автомобиля, почерк, видеозапись или фотография – вероятно персональные данные, потому что легко позволяют идентифицировать.

Адрес, семейный статус, пол, гендер, сведения с электронных кошельков, информация о состоянии здоровья, сведения о просмотренных страницах, поисковых запросах, постах в социальных сетях – персональные данные, когда известно к кому именно они относятся.

Без идентификатора информация становится анонимной. Относящаяся информация будет представлять собой персональные данные только в случаях, когда можно провести дополнительное «расследование», не используя специальные устройства и без чрезмерных затрат времени и сил.

То есть, если у нас нет разумной возможности идентифицировать субъекта данных, то такая информация является не персональной, а анонимной.

На основе всего вышесказанного прайваси-эксперт Сергей Воронкевич, CIPP/E, CIPM, CIPT, MBA, FIP, создал авторскую формулу персональных данных.

К персональным данным относится информация, описывающая субъекта данных.

Например, Ивану Купале 38 лет и он юрист. В данном случае персональная информация - это не только имя человека, но и его профессия и возраст. Допустим, что мы не знаем полного имени, но нам известно, что какому-то человеку по имени Иван в нашем городе 38 лет, эта информация будет для нас анонимной. Однако если нам сказали, что какой-то 38-летний Иван живет в нашем городе и работает в маленькой юридической фирме “Адвокатское бюро Купала и партнеры”, мы сможем легко его идентифицировать. Такая информация будет считаться персональными данными.

Data Privacy Office

Какие права получили люди благодаря GDPR?

В первую очередь новый закон принят в связи с развитием технологий, из-за которых люди могут утратить право на личную жизнь. Мы уже рассказывали о том, что такое приватность и как она рассеивается в современном мире. Теперь поговорим о правах, которыми мы, как субъекты данных, можем пользоваться по GDPR.

ПРАВО НА ДОСТУП (статья 15 GDPR)

У каждого человека есть возможность получить свои данные или доступ к ним. Речь идет не только о той информации, которую он сам предоставил, но и о той, которую компания (контролер данных) собрала о нем из других источников или даже создала сама. Кстати, здесь мы подробнее рассказали о роли контролера и процессора. При этом субъект данных может и не подозревать, что такой сбор имел место, а данное право дает возможность субъекту об этом узнать.

Благодаря праву на доступ, вы можете узнать:

- Для каких целей используются ваши личные данные.
- Кому и в какие страны передаются (а вот здесь подробнее о трансграничной передаче данных).
- Откуда получены (источники данных).
- Сколько времени хранятся ваши персональные данные.
- Есть ли у вас право на удаление, или уточнение данных, или на их «заморозку» (ограничение обработки), а также на подачу жалобы в надзорный орган.
- Информацию о важных для вас решениях, которые принимаются автоматически.

Как компания может реализовать это право?

Она должна предоставить персональные данные в любой форме, в которой человек их запрашивает, будь то электронное письмо или бумажный документ. Как альтернатива, можно предоставить доступ к персональным данным в личном кабинете. По правилам Регламента, это должно быть совершенно бесплатно. Плату можно взимать только за дополнительные копии, а также в случае явно необоснованных или чрезмерных запросов.

ПРАВО НА УДАЛЕНИЕ ДАННЫХ (статья 17 GDPR)

Другими словами, право быть забытым. Субъект вправе потребовать от компании-контролера удалить его данные. Правда, не всё так просто. GDPR предусматривает лишь несколько обстоятельств, позволяющих воспользоваться этим правом:

01 Если данные больше не нужны для той цели, для которой они собирались первоначально. Ведь, согласно принципу ограничения хранения, данные и так стоило удалить.

02 Если человек отозвал свое согласие на обработку (когда правовое основание для обработки – согласие).

03 Если данные обрабатываются незаконно. В противном случае, субъект может сразу обратиться в надзорные органы.

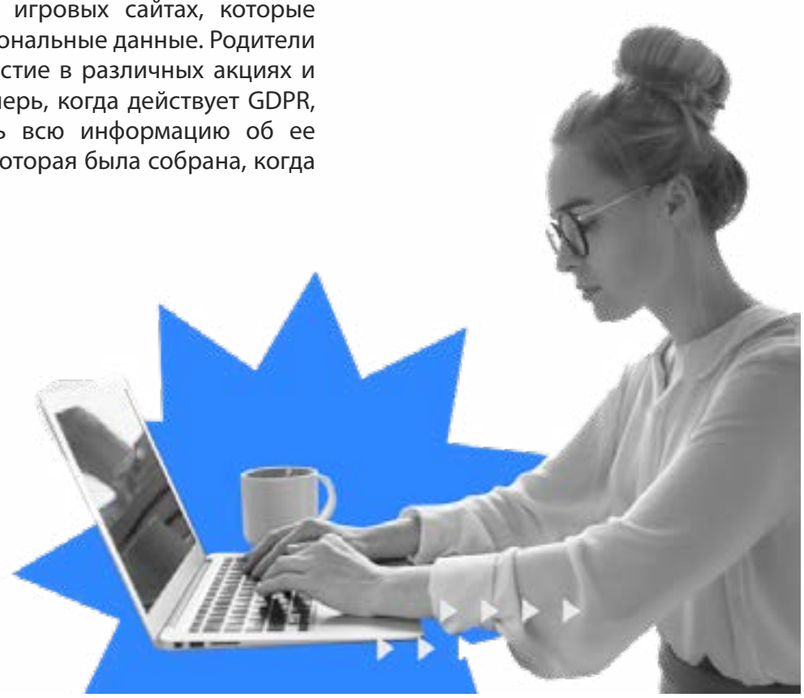
04 Если данные принадлежат ребенку и собирались онлайн-сервисом по его согласию (статья 8(1)).

Разберем подробнее последний пункт

В статье 8 Регламента говорится об обработке персональных данных детей. Согласие ребенка является действительным только если: 1) ребенку исполнилось 16 лет или 2) вместо него получено согласие/разрешение родителя. Дело в том, что дети не всегда понимают, к чему могут привести их действия в интернете. Поэтому при получении запроса на удаление подобных данных нужно немедленно это осуществить.

К праву быть забытым также есть несколько ограничений. Например, таким ограничением является право свободы слова и печати. Также под исключения попадают варианты, когда обработка данных является необходимой для целей архивирования в интересах общества, научных и исторических исследований.

Например, 22-летняя Мария заметила, что 8 лет назад регистрировалась на различных игровых сайтах, которые собирали и обрабатывали ее персональные данные. Родители подтверждали ее согласие на участие в различных акциях и розыгрышах на этих сайтах. И теперь, когда действует GDPR, Мария может требовать удалить всю информацию об ее участии в акциях и розыгрышах, которая была собрана, когда она ещё была ребенком.



ПРАВО НА УТОЧНЕНИЕ (статья 16 GDPR)

Субъект вправе потребовать корректировку информации, которая утратила достоверность или неточна, но все еще обрабатывается компанией. Такое может случиться, если он поменяет паспорт, фамилию или место жительства, или где-то в его данных была допущена ошибка. Это право становится актуальным, когда для обработки нужна точная и полная информация.

ПРАВО НА ОГРАНИЧЕНИЕ ОБРАБОТКИ (статья 18 GDPR)

Статья 18 GDPR предоставляет субъектам право приостановить использование их персональных данных по нескольким довольно редким причинам. Такие ситуации имеют место, когда:

- ставится под сомнение точность или достоверность персональных данных;
- обработка является незаконной и субъект данных возражает против удаления;
- контролер больше не нуждается в обработке персональных данных, но они необходимы субъекту для заявления, осуществления правовых исков и т. д.;
- субъект данных поставил перед контролером вопрос о том, превалируют ли легитимные интересы контролера над интересами субъекта (как только будет принято решение о возобновлении или прекращении обработки, необходимо об этом проинформировать субъекта).

«Ограничение обработки» было бы правильно перевести как «заморозка обработки». Данные все еще хранятся, но уже никак не используются.

P.S. Что такое право на доступ, право на уточнение, право на удаление данных и право на ограничение обработки, мы также разбирали здесь.

ПРАВО НА ПЕРЕНОСИМОСТЬ ДАННЫХ (статья 20 GDPR)

Субъекты данных имеют право на получение своих персональных данных в машиночитаемой форме, если это технически можно осуществить. На первый взгляд кажется, что это не отличается от права на доступ, но здесь речь идет о файлах, которые другая компания-контролер сможет импортировать в свою систему. Право на переносимость данных может быть осуществленно, если:

- основанием обработки персональных данных является согласие или договор;
- обработка должна быть автоматизированной.

Чтобы избежать утечек, машиночитаемый файл может передаваться от одного контролера к другому напрямую, без посредников. Например, социальная сеть ВКонтакте по одному клику могла бы передать все ваши альбомы с фотографиями Facebook. Пока реализовать такой механизм довольно сложно как с технической, так и с финансовой стороны. Сейчас Google, Meta, Microsoft, Twitter и Apple работают над DataTransfer Project – инициативой с открытым исходным кодом, направленной на разработку инструментов, которые обеспечат перенос данных напрямую.

Надеемся, что в ближайшем будущем все компании смогут осуществлять такую процедуру, соблюдая при этом все необходимые меры защиты.

ПРАВО НА ВОЗРАЖЕНИЕ (статья 21 GDPR)

Субъект может возразить против обработки своих персональных данных. Правда, и здесь есть свои «но». Воспользоваться этим правом можно только в том случае, если основанием для обработки выступает легитимный или публичный интерес.

Контролер обязан рассмотреть возражение, проанализировать ситуацию и принять решение: так ли важна данная обработка для компании или общественности и не превалируют ли интересы человека в данном конкретном случае?

Если субъект возражает против обработки в целях прямого маркетинга, то обработку следует прекратить НЕМЕДЛЕННО.

ПРАВО НЕ БЫТЬ ОБЪЕКТОМ АВТОМАТИЗИРОВАННОГО ПРИНЯТИЯ РЕШЕНИЙ (статья 22 GDPR)

В современном мире, при бурном развитии информационных технологий, многие решения принимаются не конкретным человеком, а с помощью автоматизированных средств. GDPR позволил субъектам возразить против решений, которые принимает компьютер без участия человека, так как в алгоритм могла закрасться ошибка или предубеждение автора.

Однако это право не действует, если:

- решение необходимо для заключения или исполнения контракта;
- решение основывается на четко выраженном согласии субъекта (explicit consent).

ПРАВО ПОДАТЬ ЖАЛОБУ В НАДЗОРНЫЙ ОРГАН (статья 77 GDPR)

Субъект вправе потребовать защиту у надзорного органа по месту жительства, по месту работы или по месту нарушения. Например, субъект, живущий и работающий в Москве, может обратиться в надзорный орган в Париже, если его права были нарушены французской компанией. Надзорный орган обязан рассмотреть жалобу и проинформировать заявителя о результатах разбирательства. Если субъекта не устраивает решение надзорного органа, он может обжаловать его в суде (статья 78 GDPR).

ПРАВО НА КОМПЕНСАЦИЮ (статья 82 GDPR)

При нарушении GDPR контролер (или процессор) обязан не только заплатить штраф, но и предоставить субъекту данных компенсацию за любой ущерб, нанесенный в результате обработки его персональных данных. Подробнее про право на переносимость, право не быть объектом автоматизированного принятия решений, право подать жалобу в надзорный орган и право на компенсацию можно почитать по ссылке.

Все вышеперечисленное подтверждает актуальность и значимость Регламента. Сегодня, в век господства науки и техники, когда интернет стал неотъемлемой частью жизни практически каждого человека, наши данные находятся далеко не в безопасности. Поэтому очень важно, чтобы каждый знал о тех правах, которыми он обладает благодаря GDPR. В таких условиях во избежание проблем с клиентами и надзорными органами компаниям необходимо информировать пользователей об их правах. Этого требуют статьи 13 и 14 GDPR. Обычно такое информирование подразумевает публикацию Privacy Policy/Notice (политика конфиденциальности или политика приватности). Мы разработали полный чек-лист по GDPR для таких политик/уведомлений.

DPO Data Privacy Office

Чек-лист для политик приватности по GDPR

1. КОНТАКТЫ КОНТРОЛЕРА

- 1.1 Наименование контролера - GDPR 13(1a), 14(1a)
- 1.2 Распределение ответственности со-контролеров: GDPR - 26(2); GoT - 44
- 1.3 Контакты контролера - GDPR 13(1a), 14(1b); GoT.Annex
- 1.4 Контакты инспектора по защите персональных данных - GDPR 13(1b), 14(1b); Annex, p.12 WP29 Guidelines on DPOs

2. ЦЕЛИ И ПРАВОВЫЕ ОСНОВАНИЯ

4. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА

- 4.1 Факт трансграничной передачи: GDPR 13(1f), 14(1f); GoT.Annex
- 4.2 Указание, обеспечивают ли страны, куда передаются персональные данные, их адекватную защиту: GDPR 13(1f), 14(1f); GoT.Annex
- 4.3 Механизмы защиты при передаче в страны, не обеспечивающие адекватную защиту персональных данных : GDPR 13(1f), 14(1f); GoT.Annex

5.ПРАВА

Принципы обработки данных

Ещё Директива 96/46/EC, предшественница Регламента, сильно изменила европейское законодательство о защите персональных данных. GDPR также внес свои поправки. Это касается и шести основных принципов обработки личной информации, которые описаны в статье 5 Регламента. Мы предлагаем разобраться в них более детально.

ПРИНЦИП ЗАКОННОСТИ, СПРАВЕДЛИВОСТИ И ПРОЗРАЧНОСТИ

Персональные данные могут быть получены только законным способом. Существует лишь шесть законных оснований для обработки персональных данных (статья 6 GDPR):

- Жизненный интерес
- Контракт
- Требование закона
- Публичный интерес
- Личный интерес
- Согласие

Прежде чем собирать данные, нужно найти в данном перечне одно правовое основание, подходящее под вашу ситуацию. Если ничего не подходит, то обработка считается незаконной. Штрафы за необоснованную обработку персональных данных довольно высокие и применяются часто.

Также, данный принцип требует, чтобы данные различных людей обрабатывались без дискриминации или обмана, то есть справедливо. Поэтому нарушением будет, если вы станете использовать информацию о модели телефона для того, чтобы выставить для их владельцев более высокие цены.

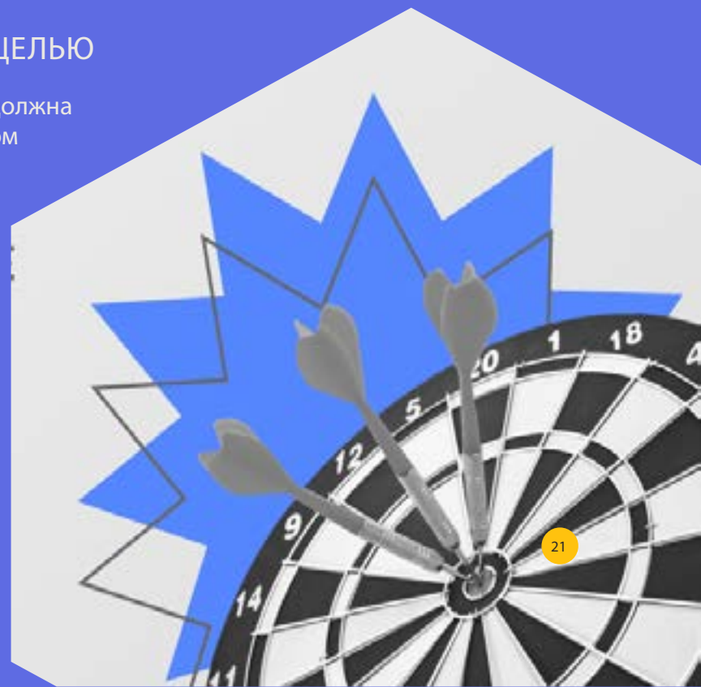
Прозрачность обработки предполагает, что людям доступна информация о целях, сроках и объемах обработки в максимально ясной и простой форме. Важно, чтобы люди, которые не имеют специальных знаний в области GDPR, могли понять, о чем идет речь. У субъектов не должно возникать вопросов: зачем и на каком основании обрабатываются их данные.

ПРИНЦИП МИНИМИЗАЦИИ ДАННЫХ

Принцип минимизации гласит, что компании не могут собирать лишние данные о клиентах. Лишние — это те данные, без которых можно достичь цель. Если вы запрашиваете информацию, чтобы доставить клиенту товар, то адреса и телефона для оперативной связи достаточно, а дата рождения будет излишней.

ПРИНЦИП ОГРАНИЧЕНИЯ ЦЕЛЬЮ

Для любой обработки компания должна назвать конкретную цель, а потом строго ее придерживаться. Например, если вы спрашиваете адрес клиента, чтобы доставить ему товар, то вы не вправе отправлять на этот адрес новогодние поздравления, поскольку это уже иная цель, которую вы не заявляли.



ПРИНЦИП ТОЧНОСТИ

Персональные данные должны быть точны и актуальны в той мере, в которой это необходимо для достижения заявленной цели. Следуя GDPR, компания должна принять все необходимые меры для обновления или удаления неверной информации. Например, если постоянный клиент меняет адрес, то мы должны исправить его в своей системе, чтобы посылка нашла адресата.

ПРИНЦИП ОГРАНИЧЕНИЯ ХРАНЕНИЯ

После достижения заявленных целей информацию следует удалить. Принцип означает, что персональные данные не могут быть использованы дольше, чем они нужны для реализации цели обработки. Например, если в вашем ресторане кто-то заказал пиццу, то уже завтра этого адреса в вашей системе быть не должно, ведь пицца доставлена (цель достигнута).

ПРИНЦИП ЦЕЛОСТНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ

Личные данные всегда представляли угрозу для своих обладателей. Но в эпоху информационного общества количество данных и уровень угроз выросли, и поэтому Регламент обязует защищать персональные данные от несанкционированного или случайного доступа, повреждения или уничтожения. И, конечно, выстраивать такую систему информационной безопасности, при которой не произойдет утечки информации, что особенно актуально в 21 веке.

НАПРИМЕР

Доставляя медицинские препараты на дом, мы обязаны скрыть от получателя имена других покупателей в списке. Например, достаточно закрыть их листочком, когда человек расписывается за доставку.

ПРИНЦИП ПОДОТЧЕТНОСТИ

Согласно статье 5(2) GDPR контролер обязан в любой момент времени быть способным продемонстрировать выполнение всех вышеперечисленные принципов. Более того, отсутствие доказательства выполнения равнозначно невыполнению.

Например, если мы не способны посредством внутренней документации, технического задания или демонстрации функционала ПО доказать, что наша система удаляет адреса, по которым мы доставляли пиццу, то мы нарушили принцип подотчетности. Надзорный орган может выписать нам штраф, не углубляясь в расследование того, действительно ли мы храним данные дольше, чем необходимо.

Надеемся, сейчас у вас сформировалось представление обо всех принципах GDPR. Однако это только первый шаг. Регламент – это не просто свод правил, которые можно выучить и универсально применять. Он имеет множество исключений, поэтому при необходимости не бойтесь обратиться к профессионалам, которые помогут во всем разобраться и построить верный маршрут на пути к правильно выстроенной системе защиты персональных данных согласно GDPR.

Территория действия GDPR

Задуматься о соответствии GDPR стоит каждой компании, деятельность которой так или иначе связана с Евросоюзом. При этом, чтобы находиться под действием Регламента, даже не обязательно иметь офисы в странах ЕС.

Сейчас объясним, как вы можете определить, нужно ли вашей компании соблюдение требований GDPR в том или ином бизнес-процессе.

Все верно, GDPR не действует на компании, а применяется к отдельным процессам («обработкам») с персональными данными. У одних компаний под GDPR окажутся все обработки, а у других – лишь некоторые процессы. Давайте выясним какие.

«Используются ли в данном процессе персональные данные?»

Положительный ответ? Тогда впереди еще пять шагов. Тем не менее, в некоторых случаях вам достаточно лишь одного «да», чтобы правила GDPR были применимы к соответствующему процессу в вашей компании.

Data Privacy Office

ВОПРОС 1.

Есть ли у вашей компании организационные единицы на территории ЕС?

Прежде чем ответить на этот вопрос, следует разобраться в понятии «организационная единица» (establishment). Согласно преамбуле 22, организационной единице не обязательно иметь статус юридического лица. Это может быть не только филиал или представительство, но и офис, удаленное рабочее место или даже один-единственный сотрудник. Если у вашей компании есть организационная единица в одной из стран Евросоюза и обработка данных связана с деятельностью этой единицы, то в таком случае применяются правила GDPR.

В качестве примера приведем дело венгерского надзорного органа Weltimmo (WELTIMMO S.R.O. V. NEMZETI A DATVEDELMI ES INFORMACIOSZABADSAGH ATOSAG). Есть компания, зарегистрированная в Словакии, которая осуществляет свою деятельность в том числе на территории Венгрии, где у нее есть почтовый ящик, банковский счет и представитель. Зашел вопрос о том, право какой страны – Словакии или Венгрии – действует в отношении деятельности компании через представителя в Венгрии в этом случае. После разбирательства Европейский суд (CJEU) решил, что всё же применимо венгерское право. Обосновали тем, что организация имеет представителя в Венгрии, пусть и не зарегистрированного в качестве филиала, отправляет и принимает почту по венгерскому адресу, пользуется банковским счетом, оформленным в местном банке, а значит осуществляет регулярную работу на территории Венгрии.

Также GDPR применим для обработок за пределами ЕС в контексте деятельности этой оргединицы, то есть процессов в вашей неевропейской компании (дочерней или материнской), тесно связанных с деятельностью европейской оргединицы. Например, в кейсе «González v. Google Spain» суд признал, что поисковая индексация как обработка персональных данных, которую производили на территории США, находится в контексте деятельности испанской оргединицы «Google Spain», а следовательно, должна соответствовать европейским нормам.

Если на вопрос этого Шага вы ответили «да», то GDPR действует на вашу обработку персональных данных и проходить остальные Шаги схемы вам не нужно. Теперь вы можете проводить через схему следующую обработку.

ВОПРОС 2.

Субъект данных находится в ЕС?

Речь идет не о гражданстве, а именно о месте нахождения субъектов. Если вы работаете с данными людей из ЕС, то переходите к Шагу 3. Если ваши субъекты находятся за пределами ЕС, то GDPR не применяется, но может применяться законодательство страны, где находится человек (например, российское, китайское или американское).

Поэтому если в вашем московском офисе работает гражданин Испании, к обработке его персональных данных будет применяться российское законодательство, но не GDPR. Остальные шаги схемы для данной обработки проходить не нужно

Если же кто-то из субъектов данных физически находится в Евросоюзе, то переходите к Шагу 3.

ВОПРОС 3.

Связана ли ваша обработка с предложением товаров и услуг субъектам, находящимся в ЕС?

Вы окажетесь на этом Шаге схемы, если ваша компания, не имеющая организационных единиц в Евросоюзе, продает товары или оказывает услуги европейцам, например, через Интернет. При этом, товары и услуги необязательно должны быть платными. К примеру, мобильное приложение, которое вы скачали в бесплатной версии, – тоже услуга.

Поскольку речь идет не о применении Регламента к компании, а к отдельной ее обработке, нужно анализировать отдельный процесс. И процессы могут быть разными, например:

- наем сотрудников в московский офис,
- восстановление пароля от онлайн-сервиса,
- ретаргетинг/ремаркетинг по посетителям, посетившим ваш сайт,
- заполнение оценочной анкеты.

В указанном выше перечне ретаргетинг/ремаркетинг является непосредственным предложением товара или услуги, оценочная анкета и восстановление пароля – связаны с оказанием услуги. Следовательно, по данным обработкам на вопрос №3 мы отвечаем «да» и переходим к Шагу 4.

А вот наем сотрудников в московский офис – это обработка персональных данных, не связанная непосредственно с предложением товаров и услуг европейцам. Предложение работы не является ни товаром, ни услугой. Поэтому по схеме мы переходим сразу к Шагу 5, где будем проверять, мониторим ли мы поведение кандидатов на должность.

Еще один пример: украинская платформа онлайн-образования продаёт свои курсы программирования на английском языке по всему миру, включая ЕС. Вопрос: нужно ли платформе соответствовать GDPR? Онлайн-курсы на данной платформе – это услуги и на вопрос №3 мы говорим: «да». Поэтому необходимо перейти к Шагу 4, чтобы выяснить, нацелена ли деятельность хотя бы на одну страну ЕС.

ВОПРОС 4.

Предусматриваете ли вы возможность предоставления товаров и услуг субъектам в ЕС?

Фактически это вопрос про присутствие на европейском рынке. Иногда может быть непонятно, применим ли GDPR, когда к вам поступил заказ от субъекта на территории ЕС. В таком случае нужно задать вопрос: «Собирались ли вы предлагать товары или услуги на территории ЕС или заказ случайный?» Ответ на этот вопрос не всегда очевиден.

Например, магазин из Москвы продает дизайнерскую одежду. Сайт компании доступен на русском и английском языках. Заказ можно оплатить в любой валюте (в том числе в евро), при этом товары доставляются по всему миру. Можно предположить, что есть таргетинг на рынок ЕС. Значит, если поступит заказ от человека, проживающего в Европейском союзе, то при обработке заказа нужно будет соблюдать требования GDPR.

Рассмотрим другой пример. Магазин, который находится в Москве, доставляет цветы по городу за российские рубли. В то же время житель Польши оформил заказ на сайте, чтобы доставить цветы своей девушке, которая живет в Москве. Поскольку магазин изначально ориентируется только на россиян и не предполагает выходить за пределы страны, то сделавший заказ поляк не будет находиться под защитой GDPR.

Таким образом, если ваш ответ на вопрос о присутствие на рынке ЕС на Шаге 4 – «да», то к вашей обработке будут применяться положения GDPR. Если же ваш ответ – «нет», то переходите к Шагу 5.

ВОПРОС 5.

Связана ли обработка с мониторингом поведения физических лиц, которые находятся на территории ЕС (например, с помощью Google Analytics)?

«Мониторинг поведения» включает наблюдение и последующий поведенческий анализ/профилирование физических лиц. В основном неевропейские компании делают это через Интернет с целью предсказать личные предпочтения людей, их поведение и отношение к чему-либо.

Следовательно, если вы осуществляете мониторинг ваших европейских потребителей, то этот процесс регулируется GDPR.

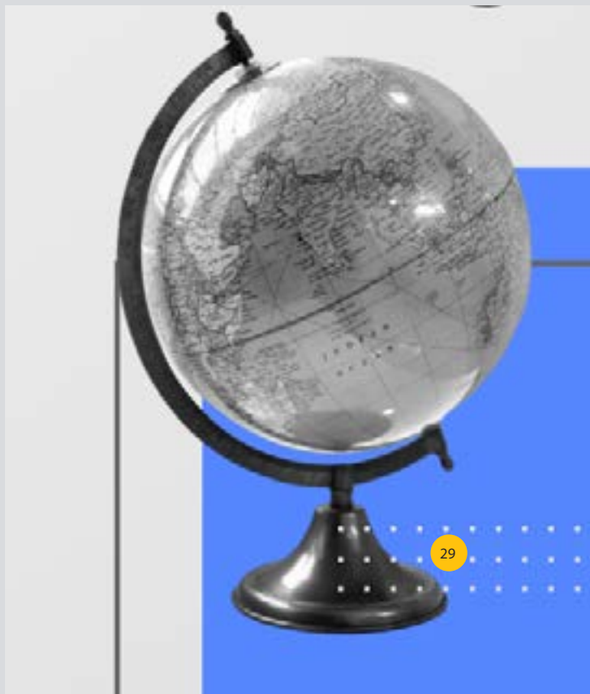
Примером мониторинга будет отслеживание поведения пользователей на сайте с помощью файлов cookies. Это позволяет предлагать им более подходящие товары или услуги, чем нередко пользуются владельцы интернет-магазинов.

Рассмотрим еще несколько ситуаций, описанных в руководстве надзорного органа.

Американская консалтинговая компания консультирует торговый центр во Франции по вопросам планировки розничной торговли. Для этого с помощью WiFi она анализирует перемещения людей по этому центру. В данном случае анализ перемещений покупателей и есть мониторинг их поведения. Поскольку торговый центр расположен во Франции, то и мониторинг относится к поведению покупателей во Франции. Поэтому к данной обработке будет применим GDPR.

Разработчик мобильных фитнес-приложений в Канаде анализирует физическую активность пользователей по всему миру для оптимизации работы и улучшения качества обслуживания. Данная обработка также регулируется европейским Регламентом.

Таким образом, если на вопрос о мониторинге вы ответили положительно, то к обработке будет применяться GDPR. Если же отрицательно, то правила Регламента не действуют, однако стоит всегда помнить о национальном законодательстве в области защиты персональных данных.



Таким образом, область применения GDPR очень широкая. Под действие Регламента попадает большое количество малых, средних и крупных бизнесов как в Евросоюзе, так и за его пределами, которые обрабатывают персональные данные своих клиентов.

Мы выделили сферы действия бизнеса, где необходимо уделить внимание правилам GDPR:

- IT-продукт и IT-аутсорс;
- банки и финтех организации;
- больницы и медицинские центры;
- онлайн-школы и хабы курсов;
- e-commerce и интернет-магазины;
- гостиничный бизнес и хостелы;
- туристические услуги и агенты;
- логистика и перевозки (авиа, авто, ж/д, морские и т. д.);
- услуги связи и телекоммуникации.

Хотя Регламент - это один из самых актуальных вопросов, который волнует предпринимателей по всему миру, соответствие GDPR можно рассматривать не как проблему, а как конкурентное преимущество. С одной стороны, компания вкладывает ресурсы в соблюдение GDPR, а с другой - получает заслуженное доверие и уважение со стороны клиентов и партнеров.

Что нужно делать по GDPR?

Очевидно, если вы дошли до этого пункта, вопрос «внедрять или не внедрять GDPR?» у вас не стоит. Давайте поговорим о конкретных действиях, которые необходимо выполнить компании, чтобы достичь compliance.

GDPR-compliance – это прежде всего выстраивание бизнес-процессов компании в соответствии с правилами Регламента. При внедрении GDPR компании зачастую используют план действий, который содержится в стандарте ISO 27701 - Управление информационной безопасностью. В него входят следующие мероприятия:

1. Выстраивание системы
2. Обеспечение безопасности данных
3. Соблюдение законности обработки данных
4. Обеспечение прозрачности обработки и прав субъектов
5. Ограничение целью, минимизация данных и ограничение срока хранения
6. Законная передача данных
7. Найм инспектора по защите персональных данных (DPO)
8. Установление и соблюдение цели обработки
9. Определение правовых оснований

Давайте рассмотрим их подробнее.

01 ВЫСТРАИВАНИЕ СИСТЕМЫ

1. Выявлять контекст организации, определять потребности организации в защите персональных данных, привлекаемых и заинтересованных в этом лиц, охвата работ. Иными словами, необходимо провести рекогносцировку на местности, выбрать союзников и сформулировать цель.
2. Заручиться поддержкой руководства компании (а здесь рассказали, как уговорить босса дать деньги на внедрение GDPR), поскольку потребуется значительное изменение в процессах и существенные затраты. Также не редкость, когда компании вынуждены ограничить себя в маркетинговой деятельности, умерить свой аппетит к объемам персональных данных.
3. Спланировать мероприятия по защите персональных данных, определить зоны ответственности различных департаментов, сотрудников.
4. На берегу договориться, как будет оцениваться эффективность программы по защите персональных данных. То есть, сформулировать индикаторы успеха, KPI.
5. Провести инвентаризацию персональных данных и информационных систем, заполнив реестр обработок персональных данных по ст. 30 GDPR (RoPA).
6. Оценить, какие есть риски для компании в связи с GDPR (штрафы, потери контрактов, сложности на отдельных рынках, лояльность клиентов). Определить, от каких именно процессов (обработок персональных данных) исходит большинство этих рисков.
7. Разработать локальные нормативные правовые акты (политики информационной приватности и безопасности) исходя из уровня рисков, вида деятельности, корпоративной культуры, организационной структуры, рынка, потребностей и других характеристик компании.

02 БЕЗОПАСНОСТЬ ДАННЫХ

8. Привести информационную безопасность компании к должному уровню. Для этого необходимо не только разработать положение об информационной безопасности, но и:

    - назначить ответственных за безопасность лиц, наделить их необходимыми полномочиями либо выделить отдел по информационной безопасности;
    - выстроить работы по контролю за информационными активами;
    - разработать правила использования мобильных устройств и удаленной работы;
    - обеспечить управление доступами к персональным данным;
    - проводить скрининг сотрудников, внутренних и внешних аудитов;
    - шифровать данные;
    - управлять инцидентами;
    - обеспечить физическую защиту данных;
    - согласовать приобретение новых систем;
    - подключать новых подрядчиков и вести их мониторинг.

Data Privacy Office

03 ЗАКОННОСТЬ ОБРАБОТКИ ДАННЫХ

9. Выделить, структурировать и задокументировать все цели обработок персональных данных. Необходимо сформулировать цели не юридическим, а «человеческим» языком, причем настолько конкретно и ясно,
    - чтобы можно было выделить в процессах различные обработки (processing activities) по GDPR;
    - чтобы можно было подобрать одно-единственное правовое основание под каждую обработку;
    - чтобы типичный представитель вашей целевой аудитории мог понять из формулировки, что будет происходить с его персональными данными.
10. Правильно подобрать одно из шести правовых оснований для каждой цели/обработки персональных данных, проставив в Реестре обработок (RoPA) по одному правовому основанию напротив каждой строки/обработки. В случае если основание – согласие, необходимо сформулировать и задокументировать его. Потом также придется выполнить требования ISO27701.7.2.4, запустив процесс сбора согласия, ISO27701.3.4 – изменения или отзыва, и ISO27701.2.3 – процесс доказывания его предоставления. Если же основание – легитимный интерес, необходимо очертить его рамки, усилить с помощью мер предосторожности (safeguards) и задокументировать данный интерес, проведя Оценку легитимного интереса (Legitimate Interest Assessment) и затем реализовав меры предосторожности, выбранные в Оценке. Если основание – требование закона, необходимо найти соответствующую норму, обязывающую обрабатывать персональные данные, и сослаться на нее в Реестре обработок.
11. Если среди обрабатываемой информации есть также биометрические, медицинские и другие специальные категории персональных данных, то наряду с правовыми основаниями обработки придется также найти одно из исключений по ст. 9(2) GDPR, которое позволяет снять запрет на обработку персональных данных для данной цели.
12. Среди всего перечня обработок, которые ведет компания, необходимо найти все обработки, в которых правовым основанием является согласие. Далее необходимо убедиться, что компания будет способна продемонстрировать надзорному органу, аудитору или субъекту данных, что она действительно получала согласие на обработку данных. Вместе с доказыванием факта получения согласия потребуется фиксировать обстоятельства его получения (время, место дачи согласия, а также его содержание).
13. Получать и регистрировать согласия на обработку персональных данных от субъектов. Они могут быть получены в электронной, бумажной или устной форме. Но даже в случае устного согласия, необходима регистрация этих согласий в соответствующем логе, журнале или карточке клиента. Учтите, что согласие необходимо получать не для всех обработок. Это не единственное основание: отказ о другого правового основания (например, контракта или легитимного интереса) в пользу согласия может быть нарушением GDPR.
14. Проводить оценку воздействия на защиту персональных данных (DPIA) для отдельной обработки персональных данных, когда в ее результате скорее всего материализуется серьезный с точки зрения последствий риск. Причем учтите, что риск оценивается не для вашей компании, а с точки зрения последствий для субъекта персональных данных, его прав и свобод. Необходимо руководствоваться ст.35 GDPR и Руководством о DPIA.

15. Связывать обязательствами всех подрядчиков, которым передаются персональные данные. Для этого нужно подписать Data Processing Agreement в соответствии со ст.28 GDPR. Соглашение должно содержать все положения, упомянутые в ст.28(3), а также перечень мер информационной безопасности, чтобы обеспечить целостность, конфиденциальность и доступность передаваемых персональных данных.
16. Выявить процессы, в которых компания совместно с кем-то еще определяет цели и средства обработки, и заключить один или несколько договоров с со-контролерами. Роли и обязанности со-контролеров должны быть задокументированы в контракте или любом аналогичном обязательном документе, который содержит условия совместной обработки данных.
17. Разработать, наполнить и поддерживать в актуальном состоянии Реестр обработок персональных данных по ст.30 GDPR (RoPA). Он представляет собой каталог целей обработки данных, а также содержит в себе сведения о собираемых данных, процессорах, сроках удаления и т.п. Именно с Реестра обычно начинаются проверки и аудиты по GDPR. Он помогает оперативно отвечать на запросы субъектов данных, так как облегчает поиск их данных среди департаментов и информационных систем.

04 ПРОЗРАЧНОСТЬ ОБРАБОТКИ И ПРАВА СУБЪЕКТОВ

18. Определить и задокументировать, в каких точках субъект данных может ознакомиться с privacy notice / privacy policy для каждой обработки. Это не сводится лишь к политике на сайте. Необходимо предусмотреть способы информирования при офлайн-взаимодействии (в офисе или на мероприятиях), а также при разговорах по телефону. Аналогично необходимо определить, какие из прав GDPR есть у субъекта в контексте каждой обработки (каждого процесса) и каким образом субъект сможет реализовать свои права онлайн на сайте, в приложении, при полученииe email, смс, push-уведомлений, бумажных рассылок, либо когда ваш сотрудник беседует с ним по телефону. Например, необходимо определить, имеется ли у человека право быть забытым в данном процессе и каким образом он будет при необходимости запрашивать копию своих персональных данных.
19. Если ваша компания принимает автоматизированные решения, которые могут иметь серьезные последствия для субъектов данных, вам необходимо определить, какие обязательства возникают у вас перед людьми в связи с тем, что эти значимые решения были автоматизированы. Например, 1) уведомлять субъектов о существовании и логике автоматизированных решений, 2) снижать риски причинения вреда правам и интересам людей, 3) предоставлять им право возражать против автоматизированного решения.
20. Определить, о чем компания должна информировать людей в связи с обработкой их персональных данных. Этот потребуется для наполнения политик приватности. По перечню можно проверить, насколько полную информацию компания предоставляет субъектам данных. В GDPR эта информация указана в ст.13 и 14 GDPR, а также Guidelines on transparency. Кроме того, субъекты данных могут запрашивать информацию индивидуально. В GDPR перечень такой информации содержится в ст.15(1).
21. Предоставить с помощью политики приватности и других уведомлений четкую и легкодоступную информацию об обработке персональных данных. Например, среди всего прочего, указанного в ст.13-14 GDPR, нужно сообщать о цели, правовых основаниях, длительности каждой обработки, получателях персональных данных. Требуется назвать компанию, контакты ее DPO, а также наименования других компаний, с которыми она совместно контролирует обработку данных. Политики приватности должны быть понятны типичному представителю целевой аудитории, а значит, нужно их перевести на каждый язык интерфейса, избавиться от юридического сленга, публиковать информацию в визуально наглядной форме, например, форматировать и структурировать текст, добавлять иконки, картинки, видео, таблицы и подсказки. Также стоит сделать удобную навигацию, разделить бесконечную простынь текста на связные кусочки, чтобы показывать их в подходящий момент (just in time notice).

22. Разработать и внедрить процесс для отзыва согласий на обработку персональных данных. В рамках процессно-ориентированного подхода необходимо определить «клиентов» процесса, его цели и результаты, показатели эффективности и необходимые ресурсы, поставщиков, исполнителей и владельца процесса отзыва или изменения согласия.
23. Разработать и внедрить процесс анализа возражений против обработки, которая ведется на основании легитимного или публичного интересов. Здесь же предполагается рассмотрение индивидуальных запросов и возможность отказа в реализации данного права, если запрос необоснованный.
24. Разработать и внедрить бизнес-процесс реализации прав на доступ, исправление и удаление персональных данных.
25. Разработать и внедрить процесс уведомления сторонних организаций и лиц, получивших от компании персональные данные, что субъект воспользовался своим правом на отзыв, исправление данных или возражение против их обработки. Это требуется, чтобы получатели могли самостоятельно решить, нужно ли им также удалять, блокировать или изменять информацию.
26. Подготовиться к запросам субъекта на 1) доступ к его (ее) персональным данным (обращению за их копией) в человеко-читабельном виде, а также 2) переносимость данных в машино-читабельной форме: определить объем выгрузки и задействованные информационные системы, а также внедрить соответствующий бизнес-процесс.
27. Разработать и задокументировать процедуры того, как компания будет отвечать на запросы субъектов персональных данных без неоправданной задержки, но не позже одного месяца.

05 ОГРАНИЧЕНИЕ ЦЕЛЬЮ, МИНИМИЗАЦИЯ ДАННЫХ И ОГРАНИЧЕНИЕ СРОКА ХРАНЕНИЯ

28. Свести объем собираемых данных к минимально необходимому для конкретной цели обработки.
29. При работе с данными, которые оказались в информационной системе организации, необходимо своевременно удалять ненужные сведения, сокращать круг лиц, имеющих к ним доступ.
30. Определить, какая точность необходима для каждой из обрабатываемых категорий персональных данных с точки зрения заявленной организацией цели. Для тех данных, точность которых важна, следует разработать процедуру изменения (например, ошибок в именах) и регулярной актуализации устаревающих данных (например, адресов или телефонов).
31. По возможности использовать анонимные данные. С помощью Реестра обработок компания должна «навести порядок» в информации: какие из сведений для каких конкретных целей используются? После этого требуется проследить, чтобы эти сведения не использовались для иных целей.
32. Необходимо предусмотреть технические или организационные механизмы удаления или полной анонимизации персональных данных после истечения сроков хранения данных.
33. Выявить подразделения, а также участки информационных систем, в которых в результате регулярной обработки персональных данных могут появиться дубликаты или временные файлы с такими данными. Затем необходимо разработать процедуры и правила удаления этих файлов, как только они перестали быть нужны.
34. Установить для каждой обрабатываемой категории персональных данных срок обработки или критерий его определения. Эти сроки формируют Графики или Расписания удаления данных.
35. Внедрить и задокументировать процедуры утилизации носителей с персональными данными.

06 ПЕРЕДАЧА ДАННЫХ

36. Использовать надежные каналы для передачи персональных данных, чтобы не допустить потерю личной информации или ее попадание в чужие руки.
37. Оформить трансграничную передачу персональных данных (в том числе доступа к ним) за пределы Европейского союза. Самый эффективный механизм передачи в нашем случае – это подписание Standard Contractual Clauses (Стандартные договорные условия), при этом регулярного контролируя подписавших соглашения поставщиков (опросники и выборочные аудиты).
38. Вести учет стран, в которые компания отправляет персональные данные.
39. Регистрировать передачу персональных данных каким-либо третьим лицам (процессорам, партнерам, аудиторам, госорганам и т.д.) и обеспечить, чтобы они содействовали выполнению запросов субъектов данных (например, запросов на доступ, удаление, корректировку и т.д.).

07 ИНСПЕКТОР ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ (DPO)

42. Назначить ответственного за защиту персональных данных (в отдельных случаях это обязательное условие). Процесс приведения компании к соответствию GDPR требует грамотного подхода, поэтому для достижения эффективности, лучше всего обратиться к профессионалам. Но в некоторых случаях Регламент требует наличие DPO (data protection officer) в штате. Советуем обратить внимание на опросник для найма инспектора по защите персональных данных, который разработали консультанты нашей компании, чтобы на этапе собеседования оценить профессиональные навыки, опыт кандидата и не упустить ни одного важного вопроса.

Подумайте: какое правовое основание подходит для цели №1, а какое для цели №2?

08 ОПРЕДЕЛИТЬ ЦЕЛЬ

У каждой обработки должна быть цель. Например, человек решил приобрести билет на самолет. Вы должны четко и понятно объяснить: «Мы собираем ваши паспортные данные (обработка), чтобы вы смогли приобрести билет (цель №1) и, чтобы проверить, не находитесь ли вы в черном списке для въезда в эту страну (цель №2)». Для каждой цели должно быть свое правовое основание.

Цель нужно сообщить субъектам данных в политике приватности (так называемой «политике конфиденциальности»). Затем нужно строго придерживаться заявленной цели, чтобы выполнить принцип «ограничения целью» (см. выше). В зависимости от цели находится правовое основание.

09 ПРАВОВЫЕ ОСНОВАНИЯ

Есть следующие варианты правовых оснований обработок:

- ✓ Жизненный интерес – обработка данных необходима, чтобы спасти кого-то от тяжелого увечья или смерти. Угроза должна быть реальна и актуальна на момент обработки.
- ✓ Контракт – без обработки персональных данных невозможно исполнение предмета договора (поставка товара, оказание услуги).
- ✓ Требование закона – когда обработка данных необходима в силу предписаний правовых актов.
- ✓ Публичный интерес – в случае, если общественно значимая обработка данных возложена на государственный орган, а лицо, обрабатывающее данные, помогает такому органу в обработке. Важным условием является то, что орган не справится без нашей помощи.
- ✓ Легитимный интерес – когда интересы компании превалируют над правами и свободами субъекта данных. Например, когда компания окажется под угрозой, если перестанет обрабатывать данные для конкретной цели.
- ✓ Согласие субъекта данных – разрешение человека обрабатывать данные для какой-то малозначимой для него цели, которое он дает компании. Оно должно быть добровольным, конкретным, даваться под конкретную цель. При этом человек должен быть информирован обо всех значимых аспектах использования его данных. Согласие должно быть выражено активным действием.

В примере про покупку билета на самолет и проверку по «черному списку» используются два разных правовых основания: для цели 1 – контракт, для цели 2 – требование закона.

Документы по GDPR

Какие из документов должны присутствовать в компании для соответствия GDPR? Такой вопрос часто задают нашим консультантам. Ответа на него нет и быть не может. Дело в том, что документация отражает принятые компанией меры и не требуется каким-либо нормативным актом сама по себе («документ ради документа»). Не все из мер обязательны для компаний, хотя есть и такие, которые необходимы большинству из них.

Название на английском	Название на русском
DPIA Methodology	Методика проведения DPIA
Employee Privacy Notice	Уведомление об обработке персональных данных сотрудников
Enterprise Privacy Risk Assessment	Оценка рисков нарушения приватности для предприятия
Guidelines for Data Inventory and Processing Activities Mapping	Руководство по инвентаризации персональных данных и выявлению их обработок
Incident Report Form	Форма отчета об инциденте
Information Assets for Disposal Log	Список информационных активов, подлежащих удалению
Internal Audit Checklist	Чек-лист для внутреннего аудита
Internal Audit Procedure	Регламент проведения внутреннего аудита
Internal Audit Report	Внутреннее аудиторское заключение
Joint Controllership Agreement	Соглашение о со-контроле (со-контролерстве)
Legitimate Interest Assessment (LIA)	Оценка легитимного интереса (LIA)
Letter of Appointment of Data Protection Officer (DPO)	Письмо о назначении инспектора по защите персональных данных (DPO)
Parental Consent Form	Форма родительского согласия
Parental Consent Withdrawal Form	Форма отзыва родительского согласия
Privacy or Data Protection Notice	Уведомление о приватности или обработке персональных данных
Processor GDPR Compliance Questionnaire	Опросник о соблюдении требований GDPR процессором
Project Plan for Complying with the EU GDPR	План проекта по выполнению GDPR
Register of Data Transfers	Реестр передач данных
Register of Privacy Notices	Реестр уведомлений об обработке персональных данных
Records of processing activities (RoPA)	Реестр обработок персональных данных (RoPA)

Название на английском	Название на русском
Binding Corporate Rules (BCR)	Обязательные корпоративные правила (BCR)
Bring Your Own Device Policy	Политика использования личных устройств
Business Continuity Plan	План мероприятий по обеспечению непрерывности деятельности
Contact list for Breach Response Team	Список контактов для группы реагирования на нарушения безопасности (утечки) персональных данных
Cookie Consent	Согласие на использование файлов cookie
Cross Border Personal Data Transfer Procedure	Регламент осуществления трансграничной передачи персональных данных
Data Breach Notification Letter to Data Subjects (template)	Письмо-уведомление субъекта данных о нарушении безопасности (утечке) персональных данных (шаблон)
Data Breach Register	Реестр нарушений безопасности (утечек) персональных данных
Data Breach Report	Отчет о нарушениях безопасности (утечках) персональных данных
Data Breach Response Plan	План мероприятий по реагированию на нарушения безопасности (утечки) персональных данных
Data Processing Agreement (DPA)	Соглашение об обработке персональных данных (DPA)
Data Protection Impact Assessment (DPIA)	Оценка воздействия на защиту персональных данных (DPIA)
Data Protection Policy (internal)	Политика защиты персональных данных (внутренняя)
Data Protection Officer (DPO) Job Description	Должностная инструкция инспектора по защите персональных данных (DPO)
Data Retention Policy	Политика хранения персональных данных
Data Sharing Agreement	Соглашение об обмене персональными данными
Data Subject Access Request Form	Форма запроса субъекта данных на доступ к информации
Data Subject Access Request Procedure	Процедура рассмотрения запроса субъекта данных на доступ к информации
Data Subject Consent Form	Форма согласия субъекта данных
Data Subject Change Request Form	Форма запроса субъекта данных на изменение информации
Data Subject Consent Withdrawal Form	Форма отзыва согласия субъекта данных
DPIA Register with Log of DPIA Outcomes and Implementation of Mitigating Controls	Реестр DPIA с журналом результатов оценки воздействия на защиту персональных данных и реализации мер по минимизации рисков
DPIA Threshold Assessment	Оценка необходимости DPIA

Data Processing Agreement (DPA)

DPA - это соглашение об обработке данных, в котором должны быть зафиксированы следующие условия (ст. 28 GDPR):

- объем, характер и продолжительность обработки;
- субъекты данных (указать, обрабатываются ли данные детей);
- категории данных;
- права и обязанности контролера и процессора;
- технические и организационные меры защиты;
- отношения с суб-процессорами.

Дополнением к DPA служат Standard Contractual Clauses (SCC) – стандартные контрактные условия.

Когда компания собирается передать данные из ЕС за его пределы, одного DPA может оказаться недостаточно. Для того, чтобы осуществить трансграничную передачу, сначала нужно узнать, обеспечивает ли страна адекватный (достаточный) уровень защиты данных. Если нет, то здесь можно узнать, как оформить трансграничную передачу данных.

Другими совами, в документе написано, что можно использовать эти самые SCC, утвержденные Еврокомиссией. Стандартные контрактные условия (SCC) – типовой договор, который заключается между контролером и процессором. Его форму нельзя изменить, т.к. он типовой. Однако могут возникнуть ситуации, когда необходимо прописать дополнительные условия, например, про распределение расходов на аудиты защиты персональных данных. Тогда поступаем следующим образом: компания заключает DPA с этими условиями, а SCC идёт приложением к нему.

Data protection impact assessment (DPIA)

DPIA (Data Protection Impact Assessment) – это способ систематически и всесторонне анализировать риски, вызываемые обработкой данных, а также подбирать меры защиты.

Причем обратить внимание нужно не на риски для компании, а на риски нарушения прав и свобод людей. Сюда относится, в том числе, угроза причинения психологического, физического, социального и экономического вреда субъектам данных.

Если компания понимает, что обработка данных, скорее всего, станет причиной серьезных рисков, то прежде, чем ее начинать, обязательно нужно провести DPIA. В ст. 35(3) GDPR есть примеры, когда серьезные негативные последствия наступят с большой вероятностью. В этих случаях обязательно проведение DPIA. Это, например:

- ✓ большое количество камер наружного наблюдения,
- ✓ работа с медицинскими карточками в больнице,
- ✓ расчет кредитного рейтинга,
- ✓ мониторинг рабочих устройств сотрудников и их действия в интернете,
- ✓ сбор данных о геолокации,
- ✓ использование финансовой информации для платежей.

Таким образом, Data Protection Impact Assessment является своеобразной подушкой безопасности, позволяющей выявить риски и предотвратить их. Это станет правильным вложением в будущее компании, так как защитит от проблем с надзорными органами, партнерами и клиентами.

Privacy notice (policy)

Уведомление о приватности (privacy notice) или политика приватности (privacy policy) - это открытый документ, рассказывающий про судьбу персональных данных, которые доверяет клиент. В нем, например, объясняется, какие персональные данные обрабатываются компанией, а также кому они передаются. Споры о том, какой перевод вернее: политика приватности или политика конфиденциальности, идут до сих пор. Мы считаем, что термин «политика конфиденциальности» неправильный, поэтому рекомендуем не называть так свои документы.

Раньше, до широкого распространения GDPR, понять текст документа могли только юристы: много сложных терминов и конструкций. Сегодня, согласно одному из требований Регламента (ст. 12 GDPR), компания обязана проинформировать пользователей не юридическими канцеляризмами, а кратко, прозрачно, понятно и без использования сложной терминологии (интерактивность только приветствуется). Далее мы расскажем, что и как нужно писать в политиках приватности с учетом статей 12, 13 и 14 GDPR.

Существуют небольшие различия в требованиях в зависимости от того, собирает ли компания персональные данные напрямую от субъекта данных или через посредников (получателей). Рассмотрим каждый из случаев.

01 Если компания собирает персональные данные от физического лица напрямую, она обязана включить в политику следующую информацию:

- ✓ название и контактные данные компании, ее представителя и инспектора по защите данных;
- ✓ цели обработки персональных данных и их правовые основания, в том числе легитимные интересы организации;
- ✓ детали, касающиеся трансграничной передачи и механизма защиты данных;
- ✓ период хранения данных;
- ✓ права субъектов данных;
- ✓ существование автоматизированной системы принятия решений, включая профилирование;
- ✓ требует ли закон или договор предоставление персональных данных, а также обязательства и возможные последствия их непредоставления.

02 Если же организация получает персональные данные косвенно (через другую компанию), в политике приватности должна быть указана вся та же информация, за исключением последнего пункта. К тому же, нужно перечислить виды (категории) персональных данных, которые получены о человеке из стороннего источника, и сами эти источники.

Политика приватности – индивидуальный документ для каждой компании, поэтому шаблон политики приватности не подойдет. Консультанты Дата Прайваси Офис разработал и специальный чек-лист составления политики приватности, который поможет вам ничего не упустить, когда вы составляете privacy policy «с нуля», или проверить правильность уже созданного

Legitimate Interest Assessment (LIA)

LIA (Legitimate Interest Assessment) – оценка легитимного интереса. Если вы работаете с персональными данными на базе такого правового основания, как легитимный интерес, то обязательно нужно сделать его оценку. Это и формальная процедура, и документ с четко регламентированным содержанием. В нем нужно взвесить все «за» и «против» обработки как для компании, так и для субъекта данных.

LIA проводится в три этапа:

1. Оценка наличия легитимного интереса.
2. Определение необходимости обработки.
3. Баланс интересов (интересы субъекта данных VS интересы компании).

Легитимные интересы компании стоит периодически пересматривать. Со временем в зависимости от внешних и внутренних факторов цель, характер или контекст обработки могут измениться. Есть большая вероятность, что это повлияет на баланс между компанией и субъектом данных. Следовательно, следует обновить LIA соответствующим образом или даже провести заново.

Эта процедура помогает избежать проблем в будущем и укрепить доверие со стороны клиентов, при этом не в ущерб самой организации.

С чего начать?

После того, как вы определили, что...

- ✓ вы обрабатываете персональные данные,
- ✓ ваши действия охвачены GDPR,
- ✓ вы контролер или процессор (хмм, а кем является почтовая служба?)...

... наступила пора выполнить вышеописанные правила как на уровне отдельных процессов (обработок), так и на уровне всей организации.

Давайте посмотрим, что именно нужно сделать в первую очередь.

Сначала необходимо определить наилучший маршрут к соответствию GDPR для вашей компании: обучить команду или подключить внешнего эксперта.

01 Обучение. Это позволит вашим сотрудникам выполнять бóльшую часть задач, а компания сможет самостоятельно внедрить GDPR. Это произойдет с меньшим темпом и меньшей эффективностью, но компания удержит при этом все знания и весь опыт внутри себя. К тому же это самый недорогой вариант. Учтите, что выполнение GDPR – дело всей компании, а не отдельных сотрудников. Один или несколько специалистов не смогут обеспечить внедрение GDPR во всей компании. Им может не хватить времени, рабочих рук, поддержки руководства, а порой – и компетенций. Недостаток компетенций может компенсировать помощь консультантов. Ниже мы расскажем про варианты обучения.

02 Консалтинг. Он нужен, когда у вас четко определен объем работ, который нужно выполнить к какому-то дедлайну, например, к заключению договора о партнерстве, прохождению аудита или запуску продукта на европейский рынок. В такой ситуации вы хотите действовать наверняка и получить реальные результаты в самые сжатые сроки. Консалтинг подходит вам, если нужно решить вопрос соответствия GDPR как можно быстрее и вы не располагаете собственными кадровыми ресурсами для этого, но готовы привлечь стороннего специалиста. Напишите нам, чтобы обратиться за помощью. Мы всегда рядом и хотим помочь.

03 Обучение + консалтинг. Этот вариант для вас, если объем работ по защите персональных данных большой, времени очень мало, а работа над GDPR горит. Тем не менее, для вас важно сохранить опыт и знания внутри организации для реализации будущих проектов по защите персональных данных. Здесь потребуется мобилизация персонала компании, а также привлечение сторонних консультантов.

Обучение

Сегодня не существует единой сертификации согласно 42 статье GDPR. Поэтому все сертификаты, дипломы и грамоты о «100% GDPR compliance», которые можно разместить на сайте - не больше, чем маркетинговая уловка. Несмотря на это, на просторах Интернета можно найти довольно много различных организаций, которые предлагают пройти обучение и получить сертификат, который покажет всему миру, что ваша компания соответствует Регламенту.

Зато получить сертификат может специалист (не компания). Обучив сотрудников и руководителей департаментов, имеющих дело с персональными данными, компания снижает свои риски по GDPR и повышает доверие клиентов. Начав с обучающих курсов и получения сертификатов от Дата Прайваси Офис, вы сделаете первый шаг в сторону GDPR-Compliance.

Рассмотрим подробнее программы курсов, которые предлагает команда Дата Прайваси Офис .

Курс GDPR Data Privacy Professional – самый популярный курс по GDPR в странах СНГ, который проводится с 2018 года. Обеспечит вас комплексными знаниями о GDPR, пониманием логики европейских требований в части защиты персональных данных. Подходит для сотрудников всех профилей, в том числе не юристов. Этот курс доступен как синхронно онлайн, так и в записи.

Программа основана на body of knowledge международной сертификации CIPP/E с учетом специфики СНГ, а именно необходимости углубленного рассмотрения:

- ✓ трансграничной передачи,
- ✓ территории действия GDPR,
- ✓ особенностей национального регулирования России, Беларуси, Украины.

Этот курс позволяет ответить на 80% вопросов по GDPR и сэкономить на внешних консультантах.

В программе:

- ✓ Понятие приватности.
- ✓ Законодательство.
- ✓ GDPR.
- ✓ Понятие персональных данных.
- ✓ Обработка персональных данных. Контролеры и процессоры данных.
- ✓ Базовые правила GDPR.
- ✓ Правовые основания обработки.
- ✓ Права субъектов данных.
- ✓ DPIA и управление рисками для приватности по GDPR.
- ✓ Информационная безопасность.
- ✓ Трансграничная передача персональных данных.
- ✓ Спроектированная приватность (Privacy by Design).
- ✓ Инспектор по защите персональных данных (DPO) и представитель в ЕС.

GDPR Data Privacy Manager

Курс GDPR Data Privacy Manager предназначен для людей, которые ранее прошли основной курс GDPR Data Privacy Professional (GDPR DPP), и представляет собой практическую подготовку по формированию и сопровождению полноценной системы защиты персональных данных.

В программе:

- ✓ Стандарты и фреймворки.
- ✓ Система управления и ее контекст.
- ✓ Планирование и управление.
- ✓ Политики.
- ✓ Организационные роли, обязанности и полномочия.
- ✓ Процессы и процедуры.
- ✓ Меры и контроли ISO 27701.
- ✓ Поддерживающая деятельность.
- ✓ Оценка эффективности и совершенствование.

GDPR Data Privacy Technologist

Курс GDPR Data Privacy Technologist освещает основные аспекты обеспечения приватности данных в IT-продуктах и сервисах. Он направлен на построение процессов защиты персональных данных при разработке, использовании IT-решений. Это обучение доступно только в записи.

В программе:

- ✓ Privacy vs Security.
- ✓ Законодательство в области приватности.
- ✓ Краткое техническое введение в компоненты инфраструктуры.
- ✓ Защита от технических рисков безопасности и приватности.
- ✓ Защита от организационных рисков безопасности и приватности.
- ✓ Жизненный цикл информации и её защита на всех этапах.
- ✓ Проектирование защищённых систем.
- ✓ Фрэймворки для защиты приватности и безопасности.
- ✓ Вопросы приватности современных технологий.
- ✓ Советы тем, кто собирается защищать приватность.

Коучинг по подготовке к сертификации CIPP/E

Коучинг по подготовке к сертификации CIPP/E (Certified Information Privacy Professional/Europe) - подготовка к международному экзамену в сфере информационной приватности CIPP/E под руководством сертифицированных экспертов.

Программа совпадает со списком тем для сдачи экзамена CIPP/E:

- ✓ Право на приватность и история его появления;
- ✓ Современное регулирование защиты персональных данных;
- ✓ Сфера действия GDPR;
- ✓ Принципы обработки персональных данных;
- ✓ Правовые основания для обработки;
- ✓ Права субъектов персональных данных;
- ✓ Информационная безопасность;
- ✓ Требования подотчетности;
- ✓ Трансграничная передача;
- ✓ Специфика работы надзорных органов и практика правоприменения;
- ✓ Особенности защиты персональных данных в трудовых отношениях;
- ✓ Privacy-friendly решения;
- ✓ Специфика работы инспектора по защите персональных данных.

Наши эксперты рассказали о том, как сдать экзамен и стать сертифицированным профессионалом в сфере приватности, и поделились своим опытом.

Мы уже рассказывали о том, как выбрать обучение. Каждый из курсов дает необходимые знания для развития карьеры в области защиты персональных данных в одном из трех направлений:

01

ПРОФЕССИОНАЛ

Знает правила и говорит, как их выполнять.

02

МЕНЕДЖЕР

Строит систему выполнения и реализации этих правил в компании.

03

ТЕХНОЛОГ

Реализовывает задумки менеджера в виде технической составляющей, то есть программного обеспечения, а также участвует в проектировании и внедрении приватности.

Консалтинг

Решение обратиться к консультанту особенно актуально при сжатых сроках и отсутствии права на ошибку. Он гарантирует правильность действий и даст вам их четкое обоснование. Консультанты Дата Прайваси Офис всегда учитывают особенности вашего бизнеса, а также имеющиеся ресурсы и процессы.

Клиенты Дата Прайваси Офис зачастую заказывают комплексные продукты, например GDPR Roadmap или Аутсорс DPO. Речь о них пойдет чуть ниже. Но некоторые выбирают отдельные услуги по GDPR (Аудит соответствия GDPR, Аудит политики приватности, Проведение DPIA, GDPR gap analysis, Data mapping, Privacy Engineering Team, Реестр персональных данных).

Внедрение GDPR Roadmap

Программа системного внедрения защиты персональных данных по международному стандарту ISO 27701. Подходит и IT-стартапам, и крупным банкам, и финтех-компаниям. Это возможность делегировать нам координацию проекта по приведению вашего бизнеса к GDPR-Compliance. Мы используем собственную методику «GDPR Roadmap» для быстрой организации защиты персональных данных в молодых компаниях, которые пока не могут похвастаться выстроенными процессами.

Этапы внедрения:

- ✓ Формирование privacy team (рабочей группы) для имплементации и ее обучение на основе body of knowledge международной сертификации CIPP/E.
- ✓ Определение пробелов и болевых точек, которые находятся под действием GDPR.
- ✓ Подбор и планирование подходящих мероприятий по ISO 27701 и их приоритизация.
- ✓ Оценка ресурсов на реализацию GDPR Roadmap.
- ✓ Создание плана действий проекта внедрения системы защиты приватности.
- ✓ Внедрение GDPR в процессы по принципу «устранение нарушений GDPR без ущерба для бизнес-процессов».

Аутсорс DPO

Компания получает опытного и компетентного специалиста, который способен оперативно и правильно решать вопросы по GDPR и – что не менее важно – нести за них ответственность.

Задачи DPO включают:

- ✓ Ведение коммуникации и консультация коллег по любым прайваси-вопросам.
- ✓ Координация работы над защитой персональных данных.
- ✓ Рассмотрение обращений субъектов персональных данных.
- ✓ Анализ несоответствий требованиям Регламента.
- ✓ Коммуникация с надзорными органами в любой стране ЕС и СНГ.
- ✓ Ведение реестра обработок в соответствии со ст. 30 GDPR.
- ✓ Регулярное обновление внутренних и внешних документов.
- ✓ Проведение оценки воздействия на защиту персональных данных (DPIA) для рисковых процессов.
- ✓ Менеджмент утечек персональных данных и уведомлений субъектов данных и надзорных органов.

Аутсорс Privacy Engineering Team

Сформированная команда, состоящая из сертифицированного эксперта по GDPR, архитектора ПО и, при необходимости, одного или нескольких программистов. От вас требуется лишь провести тестирование и задеплоить решения.

В задачи Privacy Engineering Team входит:

- ✓ Проведение аудита продукта/приложения.
- ✓ Помощь в составлении конкретных требований, относящихся именно к вашему продукту.
- ✓ Вовлеченность в проект вашей команды, чтобы «закрыть вопросы» GDPR. При необходимости, пересмотр вашего кода со внесением изменений.
- ✓ Проверка знаний ваших сотрудников и прокачка их навыков на конкретном продукте.
- ✓ Консультация ваших специалистов и определение задач по изменениям и доработкам для имплементации GDPR.
- ✓ Настраивание процессов разработки продуктов с точки зрения защиты персональных данных.
- ✓ Проведение финального тестирования продукта для оценки качества разработанной системы защиты персональных данных.
- ✓ Формирование и обучение внутри вашей компании аналогичной команды Privacy Engineering Team, способной в дальнейшем внедрять приватность во все ваши будущие продукты (дополнительная услуга).

Штрафы при невыполнении правил GDPR

General Data Protection Regulation – это серьезный нормативный правовой акт прямого действия, нарушение которого предусматривает серьезные санкции. Европейский Союз, стремясь гарантировать защиту персональных данных, установил достаточно суровые штрафы.

За нарушение Регламента предусмотрены штрафы в размерах до EUR 10 000 000 либо до EUR 20 000 000: величина варьируется в зависимости от статьи GDPR. Если оборот компании больше полумиллиарда евро, то максимальный штраф считается в процентах от мирового оборота за прошлый год: от 2% до 4%. Санкции устанавливает ст. 83 GDPR.

Важно еще то, что надзорные органы имеют право налагать административные штрафы как на контролеров, так и на процессоров данных. Штрафы могут идти вместо либо вместе с другими мерами, предписанными надзорными органами.

Топ-5 самых больших штрафа за время действия Регламента:

01

В январе 2019 года компания Google была оштрафована на 50 млн евро за то, что их политика приватности не соответствовала требованиям GDPR. Политика была написана на много страниц и на сложным языке, из-за чего пользователи не понимали, как обрабатываются их персональные данные. Кроме того, согласие на обработку персональных данных также не соответствовало Регламенту, поскольку за пользователей уже заранее были проставлены галочки во всех полях.

02

Компания H&M была оштрафована гамбургским надзорным органом на 35,3 млн евро. Такое решение было принято после того, как шведский масс-маркет бренд проводил мониторинг нескольких сотен своих сотрудников. В данную обработку попали данные о личной жизни работников, которые впоследствии стали доступны по всей компании.

03

Компания TIM (telecommunications operator) была оштрафована надзорным органом Италии на 27,8 млн евро. Компания совершила целый ряд нарушений, в числе которых: отсутствие согласия на маркетинговую деятельность; обращение к субъектам данных, которые просили не связываться с маркетинговыми предложениями; недействительные согласия, собранные в приложениях TIM; отсутствие надлежащих мер безопасности для защиты персональных данных; отсутствие четких сроков хранения данных.

04

Управление по защите данных Люксембурга (CNPD) оштрафовало Amazon на рекордные 746 млн евро в результате 19 страничной жалобы от французской группы по защите приватности «La Quadrature du Net» в 2018 году. В жалобе от имени более чем 10 000 потребителей указано, что Amazon манипулирует клиентами в коммерческих целях, выбирая, какую рекламу и информацию они получают.

05

Сеть отелей Marriott International, Inc оштрафовали на 20,5 млн евро. В 2016 году Marriott поглотила другую группу компаний, которая тоже была связана с отельным бизнесом. Позже выяснилось, что с 2014 года у этой группы компаний была серьезная уязвимость в системе защиты информации. В Marriott о ней узнали только в 2018 году, уже после утечки. Она коснулась 339 миллионов пользователей. Среди информации оказались банковские сведения и другие персональные данные.

Эти пять случаев только подтверждают слова о важности соблюдения Регламента. Внедрять GDPR обычно намного выгоднее для компании, чем действовать по принципу «а вдруг пронесет». Надзорные органы обычно обнаруживают нарушения благодаря недовольным клиентам, СМИ, блогерам, недовольным бывшим сотрудникам и т.д. Кроме этого, приватность становится маркетинговым дифференциатором для новых брендов и привлекает клиентов. Наконец, навести порядок у себя в системах и поставить процессы – задача, с которой рано или поздно столкнется любой бизнес, стремящийся к успеху.

Надеемся, эта статья оказалась вам полезна. Теперь вы понимаете основные правила GDPR и то, как с ними работать. Однако если вам будет тяжело справиться своими силами, то вы всегда можете обратиться за помощью к нашим экспертам. Это станет вложением в будущее вашей компании, а также конкурентным преимуществом на рынке уже сейчас. Так, будучи GDPR-Compliant, вы заработаете доверие и уважение со стороны клиентов и партнеров, что, несомненно, является ценным ресурсом для любого бизнеса.

Дата Прйваси Офис

Международная консалтинговая и тренинговая компания. Мы приводим ИТ-продукты в соответствие с глобальными стандартами приватности.

+44 744 1427 218 (Страны ЕС)
+49 5361 389 41 18 (Германия)
+7 958 498-32-48 (Россия)
+375 33 911-59-29 (Беларусь)
+380 94 710-00-99 (Украина)

Email: info@dpo.by

Facebook
Instagram
YouTube
LinkedIn
Telegram