КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

КАК жить после GDPR и ЧЕМУ мы научились за 1,5 года?

Наталья Гуляева

Партнер, глава практики
интеллектуальной собственности, медиа и технологий
Hogan Lovells (CIS)

Hogan Lovells

General Data Protection Regulation

GDPR вступил в силу 25 мая 2018 года

- Имеет **экстерриториальное действие**
- Предусматривает штрафы до 20 миллионов евро или 4% годового оборота компании

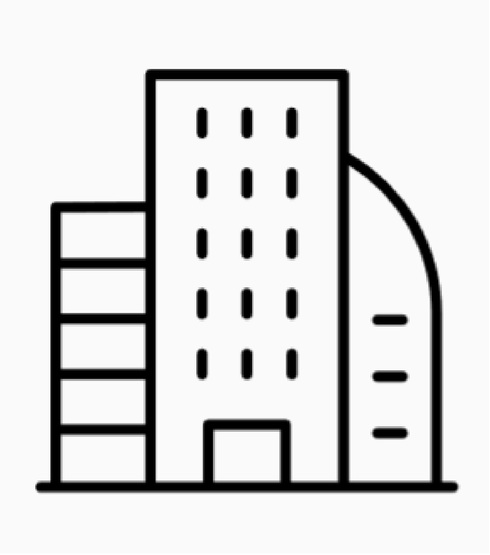
Что произошло за 1,5 года?

- Привлечено к ответственности **более 120 компаний**
- Самый крупный **штраф – 50 000 000 евро**
- Опубликовано **несколько официальных разъяснений** от регулирующих органов
- Значительно **увеличилось количество жалоб субъектов ПДн в регулирующие органы**

Сфера действия: критерий присутствия

12 ноября 2019 года Европейский совет по защите данных **утвердил Руководство по территориальному действию GDPR** в новой редакции.

1 Присутствие на территории Европейского союза



Если деятельность компании, учрежденной в ЕС, и аффилированной компании, учреждённой за пределами ЕС, неразрывно связаны, это приведет к применению GDPR, даже если такая компания в ЕС фактически не играет никакой роли в самой обработке ПДн.

Вывод о том, что субъект имеет присутствие на территории ЕС, не может быть сделан только на основании того, что его веб-сайт доступен на территории ЕС.

Сфера действия: критерий присутствия

Платформа для онлайн-торговли управляется компанией, зарегистрированной в Китае. Деятельность по обработке ПДн осуществляется исключительно в Китае.

Компания создала филиал в Берлине. Данный филиал осуществляет исключительно коммерческую и маркетинговую поддержку деятельности компании на рынках ЕС.

Критерий присутствия применяется

Сеть отелей и курортов в Южной Африке предлагает комплексные предложения через свой веб-сайт, доступный на английском, немецком, французском и испанском языках.

Компания не имеет филиалов или представительств на территории ЕС.

Критерий присутствия не применяется

Сфера действия: критерий "направленности деятельности"

2 Предложение товаров и услуг субъектам в ЕС

3 Мониторинг поведения субъектов в ЕС

Исключительно факта обработки ПДн лиц, находящихся в ЕС, недостаточно для применения GDPR. Должен присутствовать элемент "таргетирования" деятельности на лиц, находящихся в ЕС.

Для оценки поведения оператора может использоваться **критерий "направленности деятельности"**, разработанный в решениях Европейского суда справедливости по коммерческим спорам.

В частности, на направленность деятельности на рынок ЕС может указывать следующее:

- возможность размещения заказа на языке или в валюте стран-участниц ЕС,
- наличие расходов на продвижение сайта в отношении клиентов из ЕС,
- использование соответствующего доменного имени (например,".eu"),
- наличие ссылок на положительные отзывы от клиентов из стран ЕС.

Сфера действия: критерий "направленности деятельности"

Австралийская компания предлагает мобильный сервис новостей и видео контента, основанный на предпочтениях и интересах пользователей. Сервис доступен только пользователям, находящимся в Австралии (авторизация по номеру телефона).

Австралийский абонент сервиса выезжает в Германию на отдых и продолжает пользоваться сервисом.

Деятельность не направлена на рынок ЕС

Стартап, созданный в США, предоставляет приложение для туристов. Приложение обрабатывает ПДн о местоположении пользователей, как только они начинают использовать приложение, чтобы предложить рекламу ресторанов, баров и гостиниц.

Приложение доступно для туристов, когда они посещают Нью-Йорк, Сан-Франциско, Торонто, Париж и Рим.

Деятельность направлена на рынок ЕС

Сфера действия: мониторинг поведения

3 Мониторинг поведения субъектов в Европейском Союзе

Мониторинг поведения подразумевает, что контролер имеет конкретную цель для сбора и последующего использования соответствующих данных о поведении лица, находящегося в ЕС.

Европейский совет по защите данных: не каждый онлайн-сбор или анализ ПДн является "мониторингом".

Необходимо рассматривать цель контролера для обработки данных и, в частности, последующие методы поведенческого анализа или профилирования, используемые контролером.

Мониторинг выходит за рамки онлайн-отслеживания, и он также охватывает использование видеонаблюдения и обзоры рынка на основе профилей субъектов ПДн.

Практика: информирование субъектов

Управление по защите персональных данных Польши наложило **штраф в размере 943 470 злотых (приблизительно 220 000 евро)** за невыполнение обязательства по уведомлению субъектов ПДн.

Привлеченная к ответственности компания собирала данные о субъектах из общедоступных источников (например, данные из официальных реестров) и осуществляла рассылку им деловой информации.

Компания обрабатывала такие ПДн как имена, контактные данные и ID-номера более 7 миллионов человек, включая независимых трейдеров, а также людей, являющихся партнерами или членами компаний, фондов и ассоциаций.

Практика: информирование субъектов

Статья 14

Информация, которая должна предоставляться при получении персональных данных не от субъекта данных

1. В случае если персональные данные получены не от субъекта данных, контролер должен предоставить субъекту данных следующую информацию:

…

5. Параграфы 1 - 4 не должны применять в том случае, если:
…
(b) предоставление указанной информации оказывается невозможным или требует непропорционального усилия … В указанных случаях контролер должен принять соответствующие меры для защиты прав, свобод и законных интересов субъекта данных, включая доведение информации до всеобщего сведения.

Практика: информирование субъектов

Компания выполнила информационное обязательство перед почти 700 000 человек, чьи адреса электронной почты были сохранены в ее базах данных.

В отношении тех лиц, чьи персональные данные были ограничены только их почтовым адресом или номерами телефонов, **компания решила не выполнять обязательство по предоставлению информации посредством персонализированного сообщения**, поскольку это повлекло бы чрезмерно высокие расходы в размере более 33 миллиона злотых (приблизительно 7 676 миллионов евро).

Вместо этого **компания решила опубликовать информацию об обработке данных на своем веб-сайте**.

Практика: информирование субъектов

Управление по защите персональных данных Польши **не согласилось с линией защиты компании, которая была основана на статье 14 (5) (b) GDPR.**

"*Многие лица, чьи данные были обработаны компанией, не знали об этом.*

Контролер не информировал их об обработке и тем самым лишил их возможности осуществлять свои права в соответствии с GDPR".

Urząd Ochrony Danych Osobowych

В отсутствие официальных разъяснений понятия "непропорционального усилия" операторам рекомендуется принимать **все доступные меры для выполнения обязательства по предоставлению информации.**

Практика: согласие на обработку

Компания организовала лотерею, для участия в которой необходимо было указать свое имя и адрес и сделать отметки в двух окнах:

Первое окно не было предварительно отмечено и относилось к согласию на получение маркетинговых сообщений от различных третьих лиц. "Галочка" в данном окошке была необходима, чтобы принять участие в лотерее.

Второе окно было предварительно отмечено и относилось согласию пользователей на использование файлов cookie в рекламных целях, а также содержало ссылку на описание используемых файлов cookie. Пользователи могли участвовать в лотерее и сняв такую "галочку".

Практика: согласие на обработку

Чтобы согласие было действительным, оно должно быть:

"**активным**" (т. е. предполагающий конкретное действие)

"**самостоятельным**" (т. е. действие должно относиться к предоставлению согласия, а не к чему-либо еще)

"**информированным**" (т. е. субъекту должна быть предоставлена достаточная информация для понимания последствий предоставления данного согласия).

Практика: согласие на обработку

Европейский суд справедливости:

Согласие не было ни "активным", ни "самостоятельным", поскольку:

предварительно проставленной "галочки" недостаточно для получения согласия на размещение файлов cookie на устройствах пользователей

тот факт, что пользователь подтвердил участие в рекламной лотерее (дал согласие на получение маркетинговых сообщений), не является достаточным основанием для вывода о том, что пользователь дал свое согласие на установку файлов cookie или на передачу своих ПДн коммерческим партнерам

Необходимо получать отдельное согласие на обработку ПДн посредством файлов cookie.

Практика: уведомление об утечках

Статья 33

Уведомление надзорного органа об утечке персональных данных

1. В случае утечки персональных данных контролер незамедлительно и при наличии соответствующей возможности в течение 72 часов, после того как ему стало известно об утечке, должен уведомить об этом компетентный в соответствии Статьей 55 надзорный орган, кроме случаев, когда утечка персональных данных вероятно не приведет к риску для прав и свобод физических лиц.

…

Статья 34

Информирование субъекта данных об утечке персональных данных

1. В случае если утечка персональных данных может привести к высокой степени риска для прав и свобод физических лиц, контролер должен незамедлительно уведомить субъекта данных об утечке персональных данных.

Практика: уведомление об утечках

28 сентября 2018 года Facebook уведомил ирландского комиссара по защите данных об утечке.

Facebook сообщил, что он обнаружил ошибку в системе безопасности, которая позволила хакерам получить доступ к данным около 50 миллионов пользователей.

Практика: уведомление об утечках

GDPR допускает применение санкции против организации, которая столкнулась с утечкой. Выбор санкции зависит от чувствительности информации, ставшей предметом утечки.

На Facebook может быть наложен штраф в размере 1,63 миллиарда долларов США.

Поскольку причина утечки все еще расследуется ирландским комиссаром по защите данных, остается неясным, в какой степени утечка была результатом небрежности.

Расследование даст дополнительные разъяснения относительно того, как на практике распределяется ответственность за безопасность обработки и как строго наказываются нарушения.

Вопросы?

#CODEIB

natalia.gulyaeva@hoganlovells.com
+7 495 933 30 00

Источники

- https://thenounproject.com/search/?q=GDPR&i=2592955
- https://thenounproject.com/search/?q=results&i=1849426
- https://thenounproject.com/search/?q=establishment&i=2375975
- https://thenounproject.com/search/?q=purpose&i=1628799
- https://thenounproject.com/search/?q=mailing&i=1266569
- https://thenounproject.com/search/?q=check-box&i=1987068
- https://thenounproject.com/createdby_kayla/collection/sign-language/
- https://thenounproject.com/search/?q=consent&i=1830278
- https://thenounproject.com/vividzfoto/uploads/?i=1864144
- https://thenounproject.com/search/?q=questions&i=981297
- https://thenounproject.com/search/?q=cost&i=2629192

Hogan Lovells

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИТОГИ