Ежемесячник по информационной безопасности для всех

GDPR
(Основные требования по защите данных)

Обзор

Многие слышали о новом законе, называющемся GDRP или General Data Protection Regulation - Основные требования по защите данных. Этот закон был разработан Евросоюзом и вступает в силу 25 мая 2018 года. Согласно этому закону компании должны позаботится о сохранении персональных данных граждан Евросоюза, вне зависимости от того, в какой стране мира компания находится. GDPR предписывает компаниям обеспечивать безопасность и конфиденциальность персональных данных резидентов Евросоюза. Для обеспечения соответствия требованиям GDPR, необходимо понимать и применять его основные принципы.

У каждого человека есть право на приватность. Компании должны уважать это право, ограничивая количество запрашиваемых и обрабатываемых персональных данных и обеспечивая их безопасность. Эти обязательства распространяются на всю информацию о личности или её часть, которая в совокупности с другой информацией позволяет установить личность гражданина Евросоюза. Такой информацией является адрес, номер паспорта, номер водительского удостоверения, финансовая информация, биометрические данные, членство в организациях, медицинская история, место проживания, а также сексуальная, политическая или религиозная ориентация. В требованиях используется термин «natural person», подразумевающий живого человека. Вот основные тезисы этого закона:

Персональные данные должны обрабатываться в соответствии с законом, справедливым и понятным образом.

Людям необходимо объяснить, какие именно данные у них запрашиваются и с какой целью.

Персональные данные должны запрашиваться с конкретной, законной и понятной целью. Их нельзя использовать для других целей.

Персональные данные необходимо хранить и обрабатывать ровно столько, сколько они необходимы для определённой цели и не дольше.

Персональные данные должны быть актуальными и точными.

У граждан есть право получить копию их личных данных или возможность получить подтверждение, что их данные не используются и, в некоторых случаях, полностью удалены.

Организациям необходимо внедрить правила безопасности для защиты персональных данных от случайного или противозаконного уничтожения, потери, изменения или разглашения.

Компаниям необходимо обучить весь персонал, имеющий доступ к личным данным, способам безопасной работы и хранения данных.

Меры безопасности должны обеспечивать уровень защиты в соответствии со степенью секретности данных. Чем выше риск, связанный с данными, тем больше усилий должно прилагаться для защиты данных. Эти меры должны регулярно пересматриваться и, если необходимо, обновляться. Тщательно документированные решения и меры по защите и безопасности данных помогут выявить соответствие требованиям закона. Кроме того, организации должны применять такие меры, как рассмотрение контрактов, с целью обеспечения защиты персональных данных при их передаче третьим лицам или организациям, расположенным за пределами Евросоюза. В случае взлома базы данных, компании обязаны об этом сообщить в течение 72 часов от момента обнаружения утечки. При нарушении требований GDPR, компании будут оштрафованы на сумму до 4% их годового дохода. Таким образом, GDPR становится законом, нарушения которого предполагают самые высокие штрафы в мире.

Об авторе

Брайан Хонэн – *президент компании BH Consulting - независимой консалтинговой фирмы, специализирующейся на кибербезопасности и защите данных и базирующейся в Дублине, Ирландия. Брайан работал специальным советником в Europol's Cybercrime Center (EC3) – Центр по борьбе с кибер мошенничеством, Европол. Он является основателем первого в Ирландии CERT и членом совета директоров ряда инновационных компаний, занимающихся кибербезопасностью. Его страница* www.linkedIn.com/in/brianhonan *или в Twitter* @brianhonan.

Ресурсы

Обзор GDPR:	http://gdprandyou.ie
Требования GDPR:	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
Переводы и архивы OUCH!:	https://www.sans.org/u/D88

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». *Распространение журнала регулируется* Creative Commons BY-NC-ND 4.0 license. *Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь:* www.sans.org/security-awareness/ouch-newsletter. *Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова*

© SANS Institute 2018