VIII МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ»

Защита персональных данных в условиях цифрового бизнеса

09/11/2017

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

EY
Совершенствуя бизнес,
улучшаем мир

Цифровой бизнес и персональные данные

- Глобализация и развитие цифровой экономики приводят к тому, что автоматизированная обработка персональных данных составляет сегодня неотъемлемую часть операционной деятельности и имеет сложный и трансграничный характер для большинства крупных организаций
- Наличие огромных массивов разнородной информации о пользователях, обрабатываемых в огромном количестве систем и платформ, новые технологии сбора и обработки информации порождают новые потребности и услуги (планирование и формирование спроса, поведенческая реклама, адресное страхование и кредиты, облачные платформы, интернет вещей) как со стороны госструктур, так и бизнеса

Персональные данные – новая нефть?

При этом, согласно исследованию компаний Macro 4 и MaruUsurv, проведенному в UK в сентябре 2017:

- 52% (респондентов) - при наличии подозрений в обработке персональных данных какой-либо организацией без получения предварительного согласия респондента, направят в организацию запрос на предоставление разъяснений
- 39% респондентов направят подобный запрос в организацию просто из любопытства, чтобы узнать, что данная организация «знает» о них
- 26% респондентов направят подобный запрос в случае, если будет возможность получить компенсацию. (*компенсация возможна в случае, если организация не соответствует требованиям по обработке и защите ПДн или данные, обрабатываемые организацией были скомпрометированы)*
- 17% респондентов ответили, что направят подобный запрос для того, чтобы «отомстить» организациям, которые их чем-либо не удовлетворили

Ключевые тренды в обработке и защите персональных данных (1/3)

1

Усиление законодательных требований к обработке и защите персональных данных (ПДн):

- **GDPR** (General Data Protection Regulation) - вступление в силу новых требований ЕС, регламентирующих права субъектов, а также порядок обработки и защиты ПДн
- **EU ePrivacy Regulation** - новое законодательство ЕС в области защиты ПДн в электронных коммуникациях (электронный маркетинг, телеком-провайдеры, провайдеры онлайн рекламы, разработчики мобильных приложений)
- **EU-US Privacy Shield** – новые требования по трансатлантической передаче данных в рамках гармонизации с GDPR (замена устаревших требований EU-US Safe Harbor Privacy Principles)
- Изменения в национальном законодательстве Китая в области информационной безопасности и защиты ПДн
- и т.д.

Ключевые тренды в обработке и защите персональных данных (2/3)

2

Контроль за деятельностью сервис-провайдеров и партнеров по экосистеме:

- Критерий соответствия требованиям в области обработки и защиты ПДн становится одним из основных при выборе внешних сервис-провайдеров
- GDPR вводит новые обязанности и ответственность сервис-провайдеров/обработчиков ПДн

3

Внедрение концепций Privacy by design:

- Согласно результатам анализа, проведенного EY и IAPP (International Association of Privacy Professionals), наиболее зрелые с точки зрения защиты ПДн организации выполняют анализ рисков нарушения прав субъектов ПДн, а также рисков, связанных с конфиденциальностью, целостностью и доступностью ПДн, на всех этапах жизненного цикла новых продуктов/услуг/процессов/ИТ-систем (**концепция privacy by design**)

Ключевые тренды в обработке и защите персональных данных (3/3)

4

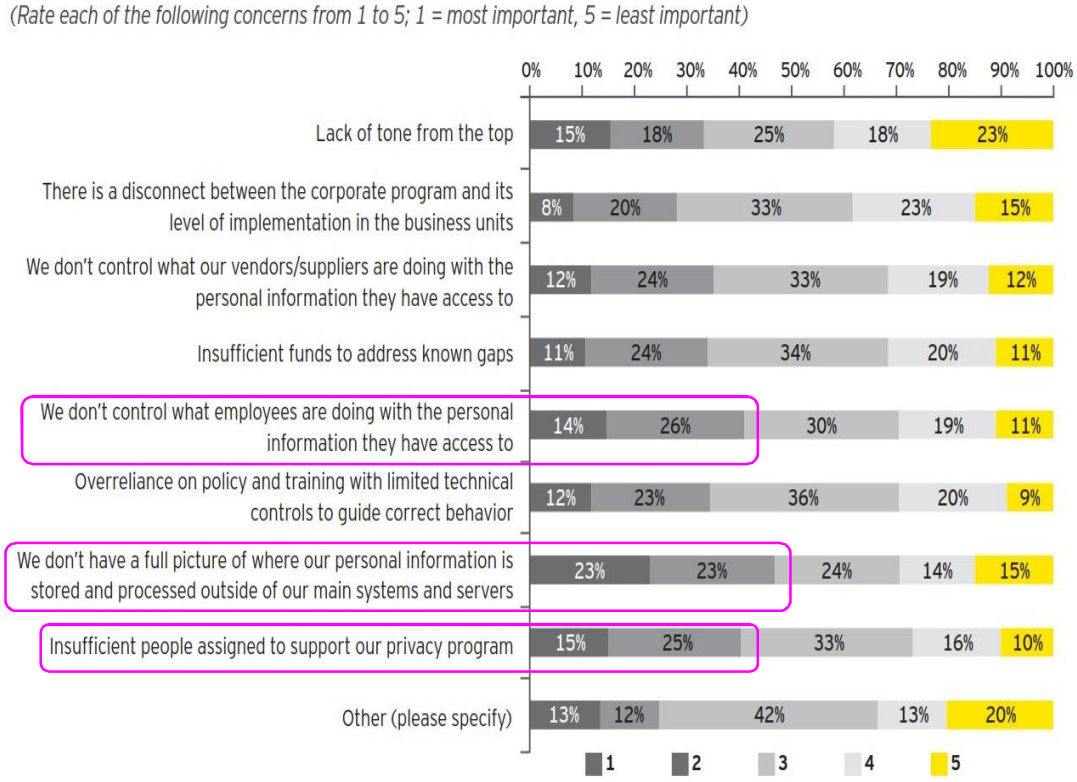
Требования по уведомлению регулятора о выявленных фактах нарушения обработки и защиты ПДн закрепляются на законодательном уровне:

- **ЕС:** GDPR предъявляет требование для операторов ПДн об информировании регулятора в течение 72 часов с момента обнаружения нарушения
- **США:** в 32 из 50 штатов существуют законодательные требования об обязательном оповещении регуляторов
- **Канада:** требование об обязательном информировании регулятора закреплено на законодательном уровне с 2015г
- **Сингапур:** требование об обязательном информировании регулятора в течение 72 часов (по аналогии с GDPR) вынесено на рассмотрение в июле 2017 г.

Основные сложности в обеспечении защиты персональных данных

По результатам ежегодного международного исследования в области информационной безопасности, проводимого EY, респондентами были сформулированы три ключевые проблемы в области защиты ПДн, представляющие наибольшую сложность для организаций:

1. Отсутствие четкого понимания где и в каком виде хранятся и обрабатываются ПДн за пределами ключевых систем и серверов
2. Отсутствие адекватных контрольных механизмов за действиями сотрудников, имеющих доступ к ПДн при исполнении служебных полномочий
3. Нехватка квалифицированных кадров и экспертизы



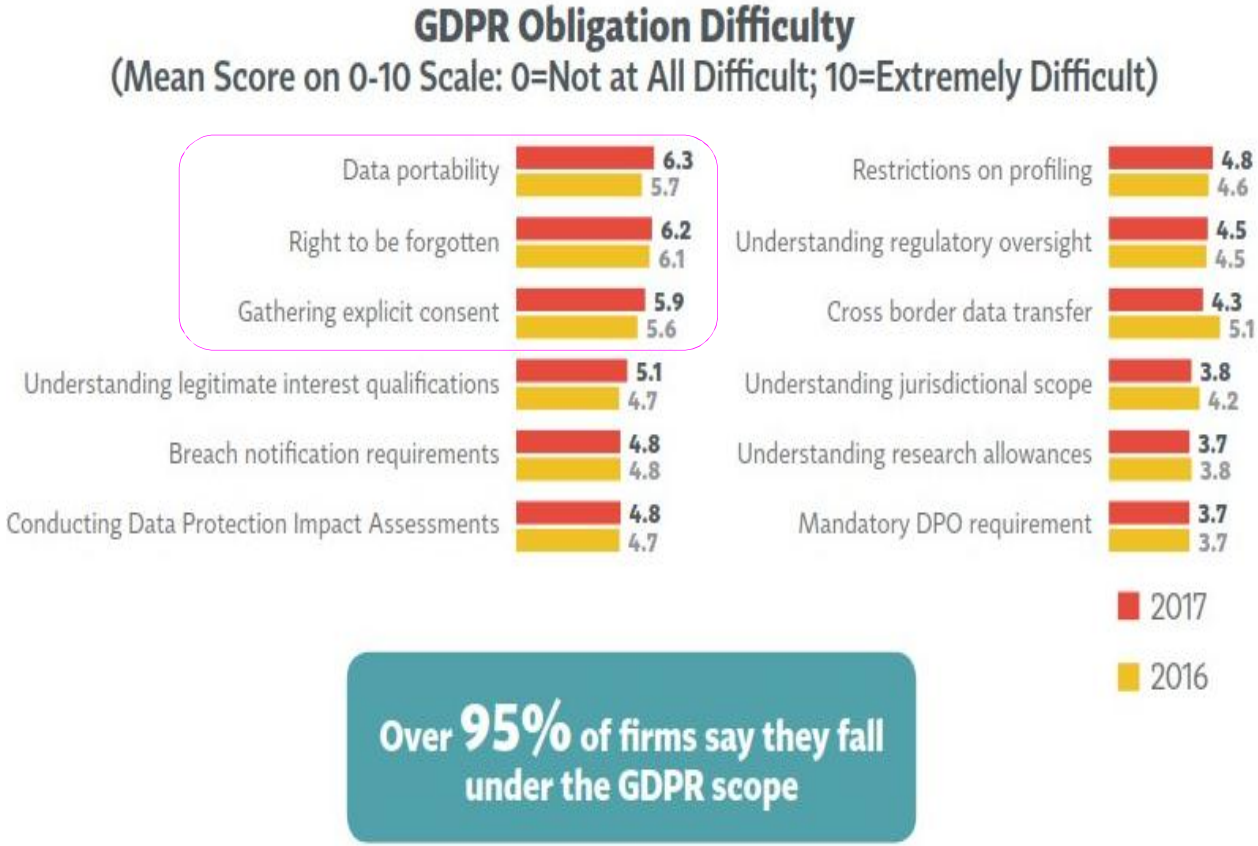
Основные сложности в выполнении требований GDPR

По результатам исследования, проведенного EY и IAPP:

- Более 95% из 548 опрошенных организаций заявили, что они попадают под требования GDPR

- Наиболее сложные для реализации требования GDPR:

1. Реализация права субъекта ПДн на перемещение данных
2. Реализация права субъекта ПДн на «забвение»
3. Получение четкого и юридически значимого согласия субъекта ПДн



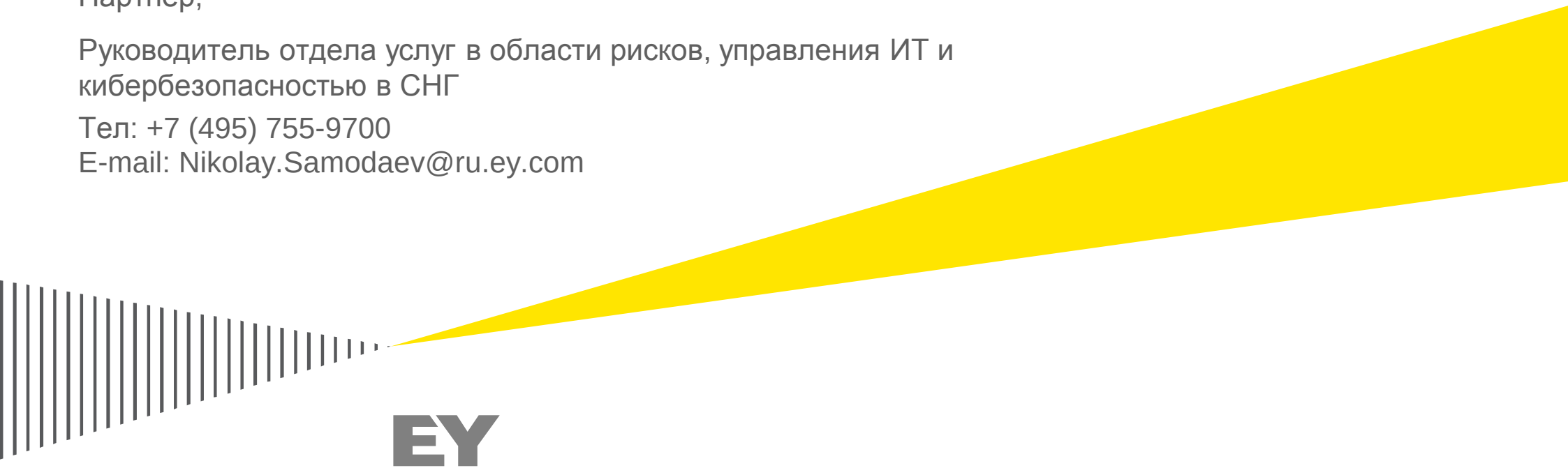
Спасибо за внимание

Николай Самодаев, CISA, MBCI

Партнер,

Руководитель отдела услуг в области рисков, управления ИТ и кибербезопасностью в СНГ

Тел: +7 (495) 755-9700
E-mail: Nikolay.Samodaev@ru.ey.com



EY
Совершенствуя бизнес,
улучшаем мир