УДК 342.9
DOI: 10.31673/2409-7292.2018.043034

В.В. Марченко, В.І. Кучер, Г.І. Гайдур

GDPR – зброя, а не захист

В статті розглянуті основні відомості про GDPR, регламент, що змінив відношення до регулювання даних в Європі та його основні проблеми. На конкретних прикладах наведені яскраво виражені недоліки створеного регламенту, з якими має зіштовхнутись кожен, хто відтепер хоче співпрацювати з ЄС. Особлива увага приділена проблемам практичної реалізації регламенту, а також використанню явних недоліків регламенту на користь зловмисника.

Ключові слова: GDPR, регламент, захист даних, штрафи, екстериторіальність, документ, індустрія, бюджет, таргетована реклама, персональні дані, вимоги, інформація, право «бути забутим», скарга.

1. Що таке GDPR?

GDPR (General Data Protection Regulation) – це Загальний регламент захисту даних, який з 25 травня 2018 року регулює збір, уніфікацію й використання персональних даних у країнах ЄС. Дія цього Регламенту поширюється й на компанії за межами ЄС, тому підприємства, які здійснюють діяльність на території Євросоюзу або в процесі своєї діяльності збирають дані громадян ЄС, повинні відповідати вимогам GDPR [1].

За текстом документу, метою GDPR є:

- Гармонізація законодавства про захист даних по всьому ЄС;
- Модернізація законів про захист даних у світлі технологічних змін;
- Посилення прав громадян;
- Збільшення вимог до відповідальності й обов’язків контролерів даних та обробників даних;
- Вдосконалення процесу створення облікових записів користувачів, а також контроль за дотриманням законів про захист даних;
- Забезпечення більшої прозорості того як використовуються дані, ким і для чого.

GDPR регулює роботу з особистими даними, які зберігаються як на електронних носіях інформації, так і в іншому вигляді. Відповідно до норм Регламенту персональні дані – це всі дані, що дозволяють прямо або опосередковано ідентифікувати особу (ім'я, IP, адреса електронної пошти, cookies, геолокація, логін, тощо).

2. Хто підпадає під дію регламенту?

Розглянемо як GDPR впливає на компанії в країнах, які не є членами ЄС. Наприклад, візьмемо компанію яка надає послуги, чи продає товари через Інтернет, в такому випадку є вірогідність, що компанія підпаде під регламент [2].

Далі, приведемо декілька питань, які допоможуть визначити чи підпадає підприємство під регламент:

- Чи націлений ваш маркетинг на користувачів ЄС? (У цьому випадку розглядається тільки таргетований маркетинг, наприклад реклама у Фейсбук для користувачів ЄС)
- Чи маєте ви клієнтів в ЄС?
- Чи маєте ви співробітників, що працюють в ЄС?
- Чи має компанія постійне представництво в ЄС?
- Чи обробляєте ви персональні дані суб’єктів, які знаходяться в одній з країн ЄС?
- Чи співпрацюєте ви з компаніями, які вже втілили вимоги регламенту, в свою чергу останні та для збереження свого статусу повинні обирати підрядника за тим самим принципом.

Якщо на будь-яке з питань ви можете відповісти так, то компанія підпадає під дію регламенту. Також, якщо Ви приймаєте платежі в євро, то Вам також прийдеться зштовхнутись з вимогами GDPR.

3. Чому нас має це турбувати?

Перш за все, регламент буде стосуватись різних міжнародних проектів, наприклад благодійні проекти з перешкоджання торгівлі людьми, наркотрафіку, наприклад Polaris Project, Slavery Footprint, International Justice Mission та багато інших.

По-друге GDPR здається створеним більш для того, щоб змусити приватний сектор бізнесу витрачати гроші на IT та поповнювати бюджет за допомогою величезних штрафів. До такого висновку можна прийти проаналізувавши інформацію в джерелах [3] та [4]. Доволі доречно згадати, що розмір штрафу за невиконання регламенту складає до 4% від річного обороту або 20 мільйонів євро. Не дивлячись на те, що це верхня межа штрафу, яскравим прикладом стане компанія UBER, яка нещодавно була оштрафована на 434 тисячі євро. Але також роздивимось приклад компанії British Airways, яка втратила 380 тисяч записів з персональними даними клієнтів, в такому випадку штраф може скласти 563 мільйони євро (4% від річного обороту).

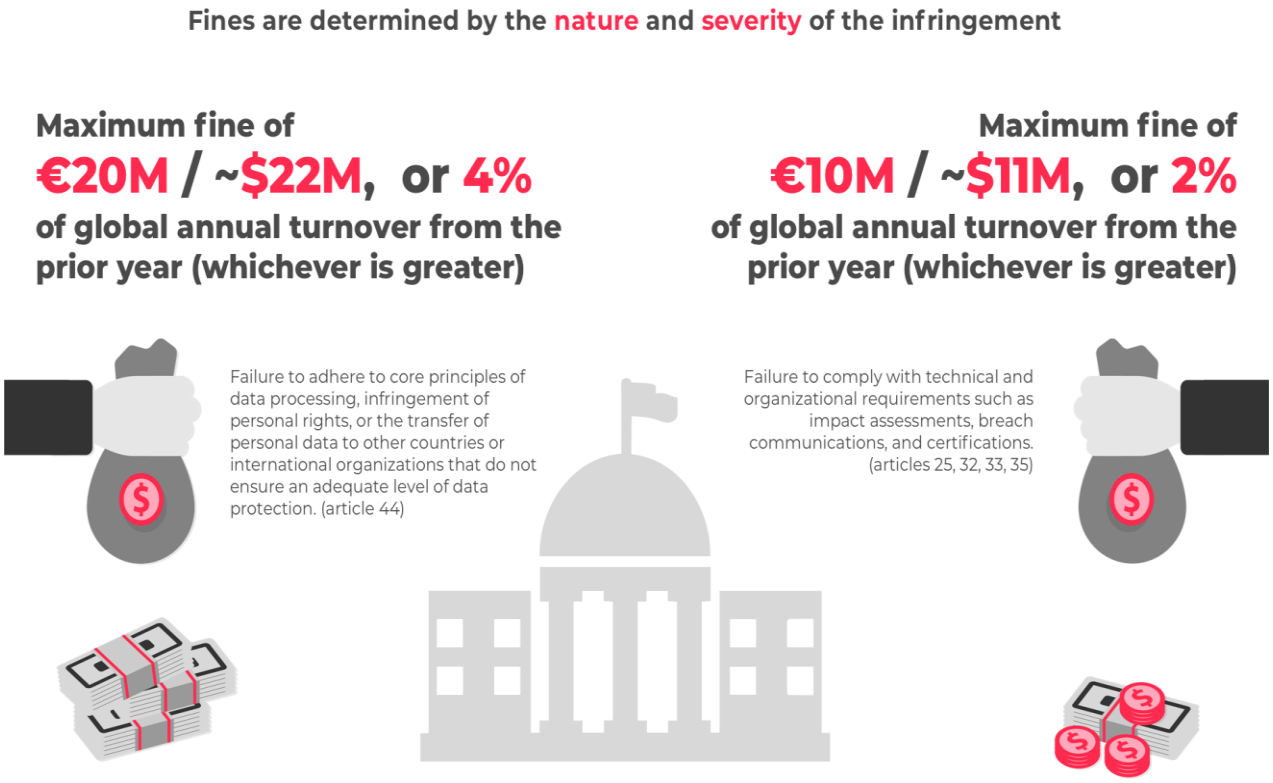

Рис. 1. Принцип розподілення частки штрафів за певні типи порушень.

До того ж, якщо перенестись на дату початку дії регламенту, гадаю кожний з нас отримував тонну електронної пошти яка інформувала Вас про те, що компанія адоптується під вимоги GDPR. Наприклад, я отримав лист від компанії до послуг якої не звертався 4 роки, і, з усього цього можна зробити прекрасний висновок – ніхто ніколи не видаляє ваші дані після отримання.

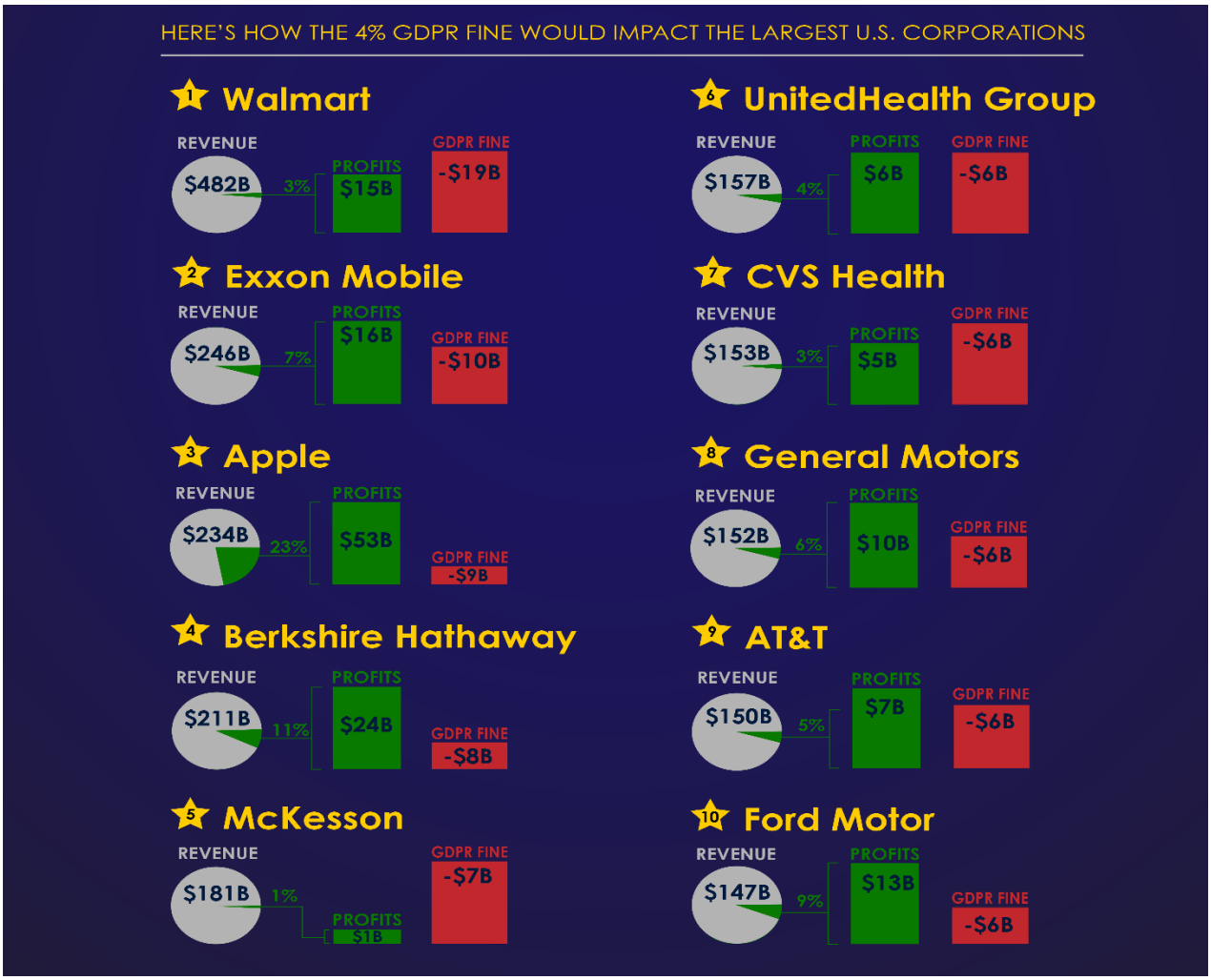

Рис. 2. Можливі штрафи на найбільші компанії США

4. Найсмачніші факти

•У регламенті присутні терміни Прямий та Непрямий, і саме тлумачення таких термінів є досить туманним. Прямі ідентифікатори включають ім'я, адресу, номер страхування, ідентифікаційний код, номер телефону, електронну пошту та біометричні записи, IP та MAC адреси та ін.. У той час як непрямим ідентифікатором є будь-які дані, які в поєднанні можуть допомогти визначити особу, наприклад комбінація статі, дати народження, географічного індикатору та інші.

•Повторюючись, під дію підпадає не тільки територія ЄС, а й компанії та особи за її територією.

•НЕ зобов'язує їх бути громадянами ЄС. До того ж не обумовлює термін «громадянство»

•НЕ вирізняє чітко різницю між групою та корпорацією.

•Державні та правоохоронні органи та деякі громадські об'єднання частково або повністю захищені. Але підрядники, сторонні вендори та незалежні експерти НЕ захищені регламентом зовсім.

•Згідно medium.com, середня вартість проведення GDPR аудиту складає 2470 євро.

•Середній час для підтримки GDPR сумісності складає 172 години на місяць, згідно medium.com.

5. Причини провалу

•Злочинці зазвичай не слідують букві закону.

- Регламент занадто комплексний та складний до втілення.
- Недолік юрисдикції для затвердження відповідності.
- Недолік розуміння комплексності IT процесів.
- Закон здається розробленим більше для нанесення економічних збитків, аніж для захисту даних.

На ілюстрації нижче [2], наведений приклад того, як за 12 кроків досягти сумісності з регламентом. Але по кожному з цих кроків можна провести лекцію на годину, і ще величезна кількість ресурсів буде потрібна аби адоптувати навіть невеличку систему.

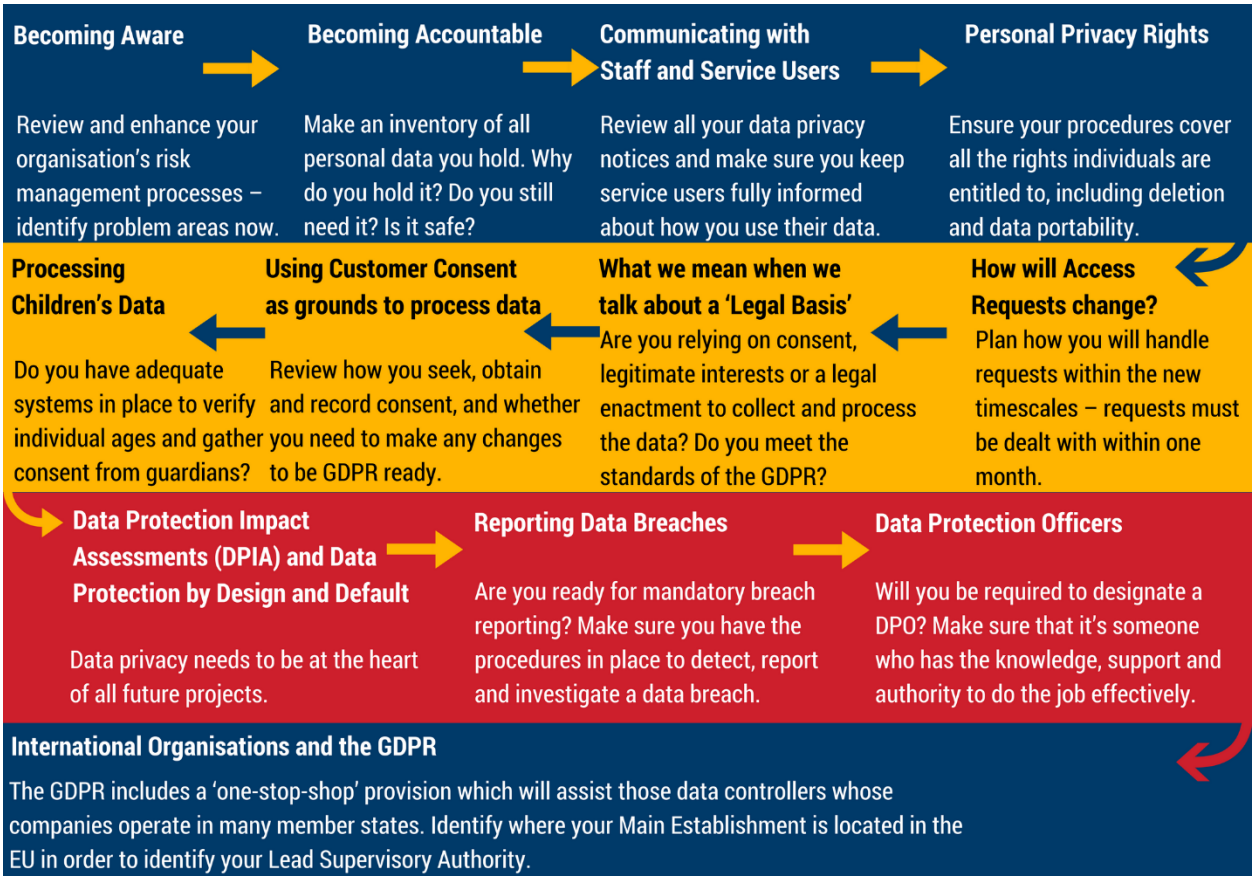

Рис. 3. Ілюстрація комплексності регламенту

6. Реакція індустрії

Перш за все регламент викликав бан користувачів з ЄС, адже набагато легше просто заборонити доступ до ресурсу, аніж втілювати GDPR. Також, вже втілені політики залишаються недосконалими та іноді навіть суперечить своїй відповідності стандарту. Але найголовнішим є те, що строгий регламент викликав відтік бізнесу з Європи, чи переведення користувачів в ЄС на спеціальні версії, помісячні платні сервіси, які інші отримують безкоштовно. Наприклад Facebook мав відокремити обробку даних для півтора мільярда користувачів, які не є громадянами ЄС і для користувачів ЄС, яких приблизно 370 мільйонів.

7. Шість кроків до «відбілення»

Отже розглянемо конкретний приклад того, як GDPR може бути використаний як зброя [5]. Уявімо що ви спеціаліст з кібербезпеки та заробляєте на хліб з маслом розробкою шкідливого програмного забезпечення, і, до усього, ви ще й громадянин ЄС. І ви хочете здаватись білим та пухнастим, отже ось що ви робите:

1. Визначаєте, які компанії, що мають відношення до безпеки або до Вас будь-яким чином мають ваші дані.
2. Надсилаєте формальне повідомлення про використання свого «права бути забутим».

3. Вичікуєте 30 днів.
4. Впевнюєтесь, чи видалені ваші дані.
5. Якщо видалені – успіх. Тепер усі докази, що були проти вас у компанії видалені.
6. Якщо ні – ви реєструєте скаргу через адвоката і передаєте діло до суду.

Ось і Все, у будь-якому випадку ви залишаєтесь у позиції переможця. Не дивлячись на те, що зберігання даних про авторів шкідливого програмного забезпечення може захистити мільйони людей, компанія матиме видалити усі зібрані дані на протязі 30 днів. Чи так має працювати регламент, направлений на захист ваших даних?

Висновки. Не дивлячись на яскраві заголовки та ідею покращити сучасний світ, GDPR є, був, і певно залишиться доволі сумнівним документом, у якому, в реаліях сучасного бізнесу та законодавства, на яскравих прикладах можна бачити реальні застосування негативних сторін регламенту. Суспільство потребує кардинально нових рішень у законодавчій сфері, які мають бути на рівень вище аніж GDPR та сповнені глибокого розуміння процесів та принципу функціонування усіх інформаційних систем. Отже, поки регламент залишається лише оскомою для усього світу, який лише ускладнив партнерство з компаніями ЄС і ми можемо лише сподіватись на те, що одного дня цю проблему перестануть ігнорувати.

Список використаних джерел

1. Arielle Pardes. WHAT IS GDPR AND WHY SHOULD YOU CARE? [Електронний ресурс] / Pardes Arielle – Режим доступу до ресурсу: https://www.wired.com/story/how-gdpr-affects-you/.
2. DATUM. What's GDPR and the penalty for non-compliance? [Електронний ресурс] / DATUM – Режим доступу до ресурсу: https://www.datumstrategy.com/blog/what-is-gdpr-fines-penalties-for-not-complying.
3. Guy Bunker. Weaponizing GDPR: when the right to erasure turns ugly. [Електронний ресурс] / Bunker Guy – Режим доступу до ресурсу: https://www.readitquik.com/articles/security-2/weaponising-gdpr-when-the-right-to-erasure-turns-ugly/.
4. Karissa Bell. Why you should care about GDPR, even if you don't live in Europe? [Електронний ресурс] / Bell Karissa – Режим доступу до ресурсу: https://mashable.com/2018/05/25/what-is-gdpr/#mXtpSdrc0aq0.
5. UISGCON 14. Logan Hicks. Weaponizing GDPR for destructive purposes [Електронний ресурс] / UISGCON 14 – Режим доступу до ресурсу: https://www.youtube.com/watch?v=ElHKUC_gtcs&t=354s.