УДК 009.4

АНАЛІЗ ВПЛИВУ ЗАГАЛЬНОГО РЕГЛАМЕНТ ПРО ЗАХИСТ ДАНИХ НА СИСТЕМИ ЗБЕРІГАННЯ ДАНИХ

А.Т. Кобевко, О.В. Тимченко

Українська академія друкарства, вул. Під Голоском, 19, Львів, 79020, Україна

Аналізуються проблеми переобладнання існуючих систем у відповідність до Загального регламенту про захист даних GDPR, відповідно змінюючи використання систем зберігання даних. Повне впровадження регламенту вимагає виконання цілого ряду технічних вимог, які на даний час ще не вирішені.

Ключові слова: *персональні дані, Загальний регламент про захист даних (GDPR), системи зберігання даних*

Постановки проблеми. Нещодавно впроваджений Загальний регламент про захист даних (GDPR) примушує багато компаній вносити значні зміни в свої системи для досягнення відповідності новим вимогам. Це регламент в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Вона також стосується експорту персональних даних за межі ЄС і ЄЕЗ. Введення нового функціоналу, який має виконуватися в реальному часі (наприклад, синхронний запис кожного запиту користувача) знижує пропускну здатність систем в 20 разів. Виникли нові технічні виклики, які необхідно вирішити, для того щоб ефективно досягти суворого дотримання Загального регламенту про захист даних. Тому для виконання Загального регламенту про захист даних потрібно внести зміни в системи обробки і зберігання даних. Проаналізувати який функціонал наявний і потрібно використовувати, а якого потрібно позбутися або поставити обмеження.

Мета статті. Дослідження проблеми переобладнання існуючих систем у відповідність законодавству, змінюючи методи використання систем зберігання даних відповідно до стандарту GDPR.

Виклад основного матеріалу. Загальний регламент про захист даних викладено в 99 статтях, які описують його правові вимоги, і 173 зведення, які надають додатковий контекст і пояснення до цих статей. GDPR є експансивним набором регулювання, що охоплює весь життєвий цикл персональних даних. Таким чином, досягнення відповідності вимагає взаємодії з компонентами інфраструктури (включаючи системи обчислень, мережі та системи зберігання даних), а також операційні компоненти (процеси, політики та персонал). Для аналізу необхідно використати статті, що описують поведінку систем зберігання даних. Вони поділяються на дві великі категорії: права суб'єктів даних (тобто людей, чиї особисті дані були зібрані) і обов'язки контролерів даних (тобто компаній, які збирають персональні дані).

В таблиці 1 показаний вплив статей Загального регламенту про захист даних на системи зберігання даних, тобто вимоги статей до функцій систем зберігання.

Таблиця 1

Основні статті GDPR, які суттєво впливають на дизайн, взаємодію або продуктивність систем зберігання даних

№	Стаття GDPR	Ключові вимоги	Функції зберігання
5.1	Обмеження призначення	Дані повинні бути зібрані та використані для конкретних цілей	Індексація метаданих
5.1	Обмеження зберігання	Дані не повинні зберігатися без потреби	Своєчасне видалення
5.2	Підзвітність	Контролер повинен мати можливість демонструвати відповідність	Всі
13	Умови збору даних	Отримайте згоду користувача для обробки даних	Всі
15	Право доступу користувачів	Надати користувачам своєчасний доступ до всіх своїх даних	Індексація метаданих
17	Право бути забутим	Пошук і видалення груп даних	Своєчасне видалення
20	Право на портативність даних	Передайте дані іншим контролерам за запитом	Індексація метаданих
21	Право на заперечення	Дані не повинні використовуватися для будь-яких обґрунтованих причин	Індексація метаданих
25	Захист дизайном і за замовчуванням	Захист і обмеження доступу до даних	Контроль доступу, Шифрування
30	Записи опрацювання даних	Зберігати логи аудиту всіх операцій	Моніторинг
32	Безпека опрацювання	Реалізація відповідних заходів безпеки даних	Контроль доступу, шифрування
33, 34	Повідомлення про порушення захисту персональних даних	Ділитися інформацією і перевіряти підозрілі системи	Моніторинг
46	Передавання з урахуванням належних гарантій	Контролюйте, де знаходяться дані	Керувати розташуванням даних

Проектування систем згідно вимог

Виходячи з аналізу статей GDPR, можна визначити шість ключових особливостей, які система зберігання повинна підтримувати, щоб бути сумісним з GDPR. А також прохарактеризувати відхилення систем в підтримці основних функцій, необхідних для виконання регламенту.

Характеристики зберігання, відповідно до стандарту GDPR

Своєчасне видалення. Згідно з GDPR не можна зберігати особисті дані протягом невизначеного періоду часу. Таким чином, система зберігання повинна підтримувати механізми TTL лічильників для персональних даних (максимальний період часу, за який пакет даних може існувати до свого зникнення), а потім автоматично своєчасно видаляти їх з усіх внутрішніх підсистем. GDPR

дозволяє TTL бути статичним часом або критерієм політики, який можна об'єктивно оцінити.

Моніторинг та логування. Щоб продемонструвати відповідність, система зберігання даних має потребу в контрольній перевірці як внутрішніх, так і зовнішніх взаємодій. Таким чином, у суворому розумінні, всі операції, незалежно від шляху (наприклад, читання або запису) або шляху управління (скажімо, зміни до метаданих або контролю доступу), повинні бути зареєстровані.

Індексація за допомогою метаданих. Системи зберігання повинні мати інтерфейси для швидкого та ефективного доступу до груп даних. Наприклад, доступ до всіх особистих даних, які можуть бути оброблені за певною метою, або експортування всіх даних, що належать користувачеві. Крім того, потрібно мати можливість швидко отримувати та видаляти великі обсяги даних, які відповідають критерію.

Управління доступом. Оскільки GDPR має на меті обмежити доступ до персональних даних тільки дозволеним установам, для встановлених цілей, а також для попередньо визначеного періоду часу, система зберігання повинна підтримувати тонкий і динамічний контроль доступу.

Шифрування. GDPR зобов'язує особисті дані шифрувати як у зберіганні так і у транспортуванні. Хоча анонімізація може допомогти зменшити обсяг і розмір даних, які потребують шифрування, але шифрування потрібне і, ймовірно, призведе до погіршення продуктивності системи зберігання.

Керування місцезнаходженням даних. Накінець, GDPR обмежує географічні місця, де можуть зберігатися особисті дані. Це означає, що системи зберігання повинні забезпечувати можливість пошуку і контролю фізичного розташування даних у будь-який час.

Ступені відповідності

Хоча GDPR є чітким у своїх високорівневих цілях, він навмисно невизначений у своїх технічних специфікаціях. Наприклад, GDPR вимагає, щоб особисті дані не зберігалися невизначений час і повинні бути видалені після закінчення терміну дії. Проте в регламенті не уточнюється, як скоро після закінчення терміну дії даних вони будуть видалені. Секунди, години або навіть дні? GDPR мовчить про це, тільки згадавши, що дані повинні бути видалені без зайвої затримки. Що це означає для розробників системи? Це те, що відповідність GDPR не повинна бути фіксованою ціллю, а спектром. Для цього враховуємо дисперсію за двома вимірами: час на відповідь і можливості.

У режимі реального часу проти можливого дотримання регламенту. Відповідність нормам реального часу - це тоді, коли система завершує завдання GDPR (наприклад, видаляє дані, що закінчили час зберігання, або відповідає на запити користувачів) синхронно, в режимі реального часу. В іншому випадку ми класифікуємо завдання як ті що треба виконати згодом. Беручи до уваги жорсткі санкції за порушення законодавства (до 4% загального доходу або 20 мільйонів євро, залежно від того, що вище), компаніям було б доцільно

видаляти дані якнайшвидше. Однак вимога задовольнити вимоги законодавства в реальному часі призводить до значних накладних витрат. Ця проблема ще більше посилюється для масштабних організацій. Наприклад, хмарна платформа Google повідомляє своїх користувачів про те, що видалені дані повинні бути повністю вилучені з усіх внутрішніх систем але це може зайняти час до 6 місяців.

Повна та часткова відповідність. Системи, які відмінні по часу реакції, демонструють різні рівні деталізації та можливості. Такі розбіжності виникають у зв'язку з тим, що багато вимог до GDPR залежать від принципів проектування та гарантій виконання певних систем. Наприклад, файлові системи не реалізують індексацію у файли як основну операцію, оскільки ця функція зазвичай підтримується за допомогою прикладних програм, таких як grep. Аналогічно, багато реляційних баз даних лише частково і опосередковано підтримують TTL, оскільки ця операція може бути реалізована з використанням визначених користувачем тригерів, які є неефективними. Таким чином, ми визначаємо повну відповідність для того, щоб підтримувати всі функції GDPR, а часткове дотримання - як підтримку функцій у поєднанні з зовнішніми інфраструктурами або компонентами.

Висновки. Проаналізувавши вплив статей (вимог) GDPR на системи зберігання, слід зазначити, що досягнення суворої відповідності є важким завданням. Наївна спроба суворого дотримання регламенту призводить до значного уповільнення роботи систем. Для кращого вивчення цього питання слід провести аналіз існуючих систем збереження даних і проаналізувати їх за наступними параметрами: ефективне логування, видалення, індексування метаданих.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cryptsetup and LUKS - open-source disk encryption. https://gitlab.com/cryptsetup/cryptsetup, Accessed May 2019.
2. Data Deletion on Google Cloud Platform. https://cloud.google.com/security/deletion/, Accessed May 2019.
3. Stunnel. https://www.stunnel.org, Accessed May 2019.
4. Anirudh Badam, KyoungSoo Park, Vivek Pai, and Larry Peterson. HashCache: Cache Storage for the Next Billion. In USENIX NSDI, 2009

REFERENCES

1. Cryptsetup and LUKS - open-source disk encryption. https://gitlab.com/cryptsetup/cryptsetup, Accessed May 2019. (in English)
2. Data Deletion on Google Cloud Platform. https://cloud.google.com/security/deletion/, Accessed May 2019. (in English)
3. Stunnel. https://www.stunnel.org, Accessed May 2019. (in English)
4. Anirudh Badam, KyoungSoo Park, Vivek Pai, and Larry Peterson. (2009),HashCache: Cache Storage for the Next Billion. In USENIX NSDI. (in English)

DOI 10.32403/2411-9210-2019-1-41-34-38

ANALYSIS OF THE INFLUENCE OF THE GENERAL DATA PROTECTION REGULATION ON THE DATA STORAGE SYSTEM

A. T. Kobevko, O.V. Tymchenko

Ukrainian Academy of Printing 19, Pid Holoskom St., Lviv, 79020, Ukraine
O_tymch@ukr.net

With the introduction of General Data Protection Regulation (GDPR) many companies were forced to make significant changes to their systems to meet the new requirements. GDPR is a regulation within the European Union legislation to protect the personal data of all people within the European Union and the European Economic Area. It also refers to the export of personal data outside the EU and EEA.

Problems of converting existing systems into conformity have been analyzed, changing the use of storage systems in accordance with the GDPR standard.

The introduction of a new functionality that should be performed in real time (for example, recording each user's request synchronously) reduces system bandwidth by 20 times. There are new technical challenges that need to be addressed in order to effectively achieve strict compliance with the General Data Protection Regulation.

Keywords*: personal data, general data protection regulation (GDPR), data storage systems*

Стаття надійшла до редакції 12.02.2019
Received 12.02.2019