Курсов проект по „Социално-правни аспекти на информационните технологии“

Какво представляват псевдонимизацията и анонимизацията в сферата на информатиката.

въведение, инструменти и технологии

Изпълнител – Цветомир Стайков, Компютърни науки, 1MI0800469

Проверил - гл. ас. д-р Калина Георгиева

Въведение

Личните данни включват информация като имена, адреси и данни за онлайн активност. Съвременните услуги изискват тяхното събиране и обработване, което поставя въпроса за условията за използването им. Проектът разглежда основните нормативни актове за защита на личните данни, методите за анонимизация и псевдонимизация и тяхното практическо приложение.

Нормативни източници

В Конституцията на Република България личните данни не са изрично дефинирани, но чл. 32, ал. 1 гарантира неприкосновеността на личния живот, част от който е информацията, разкриваща идентичността на лицето.

На международно ниво Конвенция 108/108+ установява първите стандарти за защита на личните данни, включително принципи за законност, прозрачност и защита от неправомерен достъп.

В европейското законодателство ключово значение имат Директива 95/46/ЕО, която въвежда основи на защитата на данните, и Регламент (ЕС) 2016/679 (GDPR), който я заменя. GDPR дефинира понятието „лични данни“, определя ролите на администратора и обработващия, както и принципите и задълженията при обработване.

В националната правна рамка Законът за защита на личните данни (ЗЗЛД) доразвива изискванията на GDPR и регламентира правомощията на Комисията за защита на личните данни (КЗЛД).

Към него се прилага и подзаконовият акт — Правилникът за дейността на КЗЛД и нейния административен апарат (ПДКЗЛДНА), който урежда структурата, функциите и организацията на работа на Комисията.

Компетентни органи

Комисията за защита на личните данни (КЗЛД) е независим надзорен орган, който контролира законосъобразното обработване на лични данни. Нейните функции включват извършване на проверки, разглеждане на жалби, налагане на административни санкции и издаване на указания.

Европейският комитет по защита на данните (EDPB) осигурява единното прилагане на GDPR в държавите членки, като издава насоки, добри практики и задължителни решения при спорове между националните регулатори.

Длъжностното лице по защита на данните (DPO) консултира администратора или обработващия, подпомага оценките на въздействието (DPIA) и служи като контактна точка с надзорните органи.

Субекти в обработването

„Администратор“ на лични данни е физическо или юридическо лице, което самостоятелно или съвместно с други определя целите и средствата за обработване на лични данни (чл. 4, т. 7 GDPR).

„Обработващ лични данни“ е лице, което обработва лични данни от името на администратора и по негово възлагане (чл. 4, т. 8 GDPR).

„Субект на данни“ е лице, което може да бъде идентифицирано пряко или непряко чрез различни идентификатори (чл. 4, т. 1 GDPR).

Ненормативни източници

Защитата на личните данни се подпомага от редица добри практики, технически стандарти и експертни препоръки. Становищата на Европейския комитет по защита на данните (EDPB) и други специализирани документи имат ключова роля за определяне на подходите за анонимизация и псевдонимизация.

Opinion 05/2014 на Работната група по чл. 29 представя основните техники за анонимизация и рисковете от повторна идентификация.

Оценката на въздействието върху защитата на данните (DPIA), регламентирана в чл. 35 GDPR, представлява анализ на рисковете при дейности с висок интензитет на обработване.

В технически аспект широко се използват криптографски методи като хеширане (SHA-256) и криптиране (AES-256), които позволяват ефективна псевдонимизация.

Bolognini, L., Bistolfi, C. Pseudonymization and impacts of Big Data processing in the transition from the Directive 95/46/EC to the new EU GDPR. B: Computer Law & Security Review, Том 33, Бр. 2, 2017, стр. 171–181. ISSN 0267-3649.

Самото решение

Много публични регистри са достъпни във формат CSV, което позволява лесна обработка чрез програми като Microsoft Excel. По-сложни техники могат да се реализират чрез езици като Python. Макар да предоставят свобода, тези подход изисква допълнителни знания и време за разработка.

С цел улесняване на процеса беше създаден уеб инструмент, който автоматизира обработката на CSV файлове. Приложението предлага следните функции:

- Съкращаване — трансформиране на имена в инициали.
- Хеширане — еднопосочна функция; генерира се допълнителен файл с ключ.
- Изместване — замяна на знаци със съседни
- Скриване — премахване на чувствителни стойности (анонимизация).
- Честота — извеждане на статистика за уникални стойности в колоната.
- ID-мапинг — замяна на данни с уникален идентификатор, придружен от таблица на съответствията.

Платформата е разработена с HTML, CSS и JavaScript и използва библиотеките PapaParse и Crypto.js. Достъпен е на адрес: https://www.eguardian.dev/SPAIT/

SWOT анализ

Хешированието предоставя еднопосочно преобразуване, докато изместването позволява двупосочна трансформация при наличие на необходимия ключ. ID-мапингът дава възможност за създаване на отделна таблица за съпоставяне. Скриването на данни осигурява пълна анонимизация, когато е необходимо да се елиминира рискът от идентификация.

Някои методи изискват съхранение на допълнителни елементи, като броя изместванията, криптографски ключове или таблици за съпоставяне при ID-мапинг. Това увеличава административната тежест и създава допълнителни точки на уязвимост. При метода „скриване“ съществува риск от загуба на информация.

Комбинацията от няколко метода дава възможност за създаване на различни нива на сигурност според нуждите на обработката. Частичният достъп до данните може да бъде ограничен само до лица, разполагащи с необходимите ключове или таблици, което подобрява контрола върху информацията по време на обработка.

Методи като изместването са потенциално уязвими към *brute-force* атаки, а бъдещи технологични подобрения могат да направят определени алгоритми по-лесни за разбиване. Неправилното съхранение на ключове или таблици за съответствия може да доведе до загуба на информация или до нейното изтичане.

Заключение

Темата за защитата на личните данни придобива все по-голяма значимост с появата на нови регламенти и технологични предизвикателства. Това обуславя нуждата от познаване както на нормативната рамка, така и на практическите методи за анонимизация и псевдонимизация. Разработеният уеб инструмент демонстрира как често използвани техники като съкращаване, хеширане и ID-мапинг могат да се прилагат бързо и ефективно за повишаване нивото на защита.