ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ ДІЯЛЬНОСТІ ДЕРЖАВНИХ ІНСТИТУЦІЙ

1. Нова система захисту даних для установ ЄС.

2. Особливості захисту персональних даних інституціями ЄС.

3. Особливості користування персональними даними, що були надані державним інституціям.

4. Важливість захисту персональних даних у процесі електронного урядування.

1. Нова система захисту даних для установ ЄС

Європейський Союз має нову правову базу для захисту персональних даних, які обробляються інституціями, органами, службами та агентствами Союзу. Основний Регламент (ЄС) 2018/1725 був опублікований в Офіційному журналі від 21 листопада 2018 року (L 235/39). Він скасовує Регламент (ЄС) № 45/2001 і Рішення № 1247/2002/ЄС, які відносяться до Лісабонської епохи і не охоплюють обробку персональних даних в усіх установах і органах Союзу.

Головною метою нового Регламенту є адаптація його правил до сучасного Загального регламенту захисту даних (Регламент (ЄС) 2016/679), який повністю застосовується з травня 2018 року. Отже, Регламент 2018/1725 встановлює послідовну структуру, а гарантування вільного потоку персональних даних у межах Союзу. Він також містить положення щодо Європейського інспектора із захисту даних (EDPS). ЄКЗД має право контролювати застосування положень цього Регламенту до всіх операцій обробки, які здійснюються установою чи органом Союзу. Він також є першою точкою звернення, якщо надходять скарги на порушення прав особи на захист даних.

Регламент складається з 12 розділів, серед яких:

- Загальні положення, включаючи сферу застосування та визначення;
- Загальні принципи захисту даних;
- Права суб'єкта даних;
- Контролер і обробник, включаючи положення про безпеку персональних даних;
- Передача персональних даних третім країнам або міжнародним організаціям;
- EDPS;
- Засоби правового захисту, відповідальність і штрафи;
- огляд.

Розділ IX містить спеціальні правила щодо «обробки оперативних персональних даних органами, службами та агентствами Союзу під час здійснення діяльності, яка підпадає під дію глави 4 або 5 розділу V частини третьої ДФЄС». Іншими словами, це стосується діяльності органів/служб/агенцій Союзу (як їх основних або допоміжних завдань), що здійснюються з метою запобігання, виявлення, розслідування та переслідування кримінальних правопорушень. У цьому випадку індивідуальні норми розділу IX застосовуються як lex specialis.

Слід зауважити, однак, що Регламент не застосовується до Європолу чи Європейської прокуратури до тих пір, поки не будуть внесені зміни до правових актів про заснування Європолу та Європейської прокуратури (тобто до Регламентів № 2016/794 та № 2017/1939). з метою застосування цієї глави (про обробку оперативних персональних даних) до них у адаптованому вигляді. Чи потрібно адаптувати правову основу цих установ до Регламенту, буде оцінено в процесі перегляду в 2022 році.

Правила Регламенту застосовуються з 12 грудня 2018 року, за винятком Євроюсту: Регламент застосовується до обробки персональних даних Євроюстом з 12 грудня 2019 року.

Новий Регламент, який застосовується з сьогоднішнього дня, приводить правила захисту даних для інституцій та органів ЄС (EUI) у відповідність до стандартів, які накладаються на інші організації та підприємства Загальним регламентом захисту даних (GDPR). Згідно з новими правилами, які ми можемо називати EUI-GDPR, ЄКЗД залишається відповідальним за забезпечення ефективного захисту основних прав і свобод осіб, коли їхні персональні дані обробляються інституціями ЄС або від їх імені, незалежно від того, чи це для забезпечення кращої роботи ринків ЄС, для оцінки та контролю за ліками в ЄС або для боротьби з тероризмом та організованою злочинністю». Інституції ЄС повинні брати приклад у забезпеченні захисту особистих даних.

2. Особливості захисту персональних даних інституціями ЄС.

Усі персональні дані в електронному форматі (електронна пошта, документи, бази даних, завантажені пакети даних тощо) зберігаються на серверах Європейської комісії або її підрядників. Усі операції з обробки виконуються відповідно до Рішення Комісії (ЄС, Євратом) 2017/46 від 10 січня 2017 року щодо безпеки комунікаційних та інформаційних систем у Європейській Комісії.

Підрядники Комісії пов’язані спеціальним договірним положенням щодо будь-яких операцій з обробки ваших даних від імені Комісії, а також зобов’язаннями щодо конфіденційності, що випливають із транспозиції Загального регламенту захисту даних у державах-членах ЄС (Регламент «GDPR» (ЄС).) 2016/679).

З метою захисту ваших персональних даних Комісія вжила ряд технічних та організаційних заходів. Технічні заходи включають відповідні дії щодо безпеки в Інтернеті, ризику втрати даних, зміни даних або несанкціонованого доступу, беручи до уваги ризик, пов’язаний з обробкою, і характер персональних даних, що обробляються. Організаційні заходи включають обмеження доступу до персональних даних лише для

уповноважених осіб, які мають законну потребу знати для цілей цієї операції обробки.

Зібрані персональні дані та вся пов’язана інформація зберігаються на серверах підрядників під час впровадження та обслуговування веб-сайту.

Персональні дані в електронній формі: доступ до ваших особистих даних, а також будь-якої іншої інформації, зібраної на веб-сайті, надається виключно через систему ідентифікації з паролем, доступну для обмеженої кількості користувачів, без шкоди для можливої передачі цих даних у майбутньому до органів, на які покладено контроль та перевірку діяльності Комісії відповідно до права ЄС.

Веб-сайт використовує файли cookie.

Файли cookie — це фрагменти тексту, створені веб-службами, які відвідав користувач; ці текстові файли можуть бути встановлені на пристроях користувачів веб-сайтом, який вони зараз відвідують («основні постійні файли cookie»), або іншим веб-сайтом, відмінним від того, який вони зараз відвідують («сторонні файли cookie»). Щоб полегшити роботу нашого веб-сайту, ми можемо – за згодою відвідувачів – розміщувати на вашому пристрої невеликі файли даних, які називаються файлами cookie. Вони дозволяють веб-сайту запам’ятовувати ваші дії та параметри (наприклад, ім’я для входу, мову, розмір шрифту та інші параметри відображення) протягом певного періоду часу, тож вам не потрібно вводити їх повторно, коли ви повертаєтеся на сайт або переглядати з однієї сторінки на іншу.

Використовуватимуть чотири різні типи файлів cookie:

- Основні постійні файли cookie
- Файли cookie технічної сесії
- Файли cookie третіх сторін (включаючи файли cookie Google Analytics)

- Сторонні файли cookie з віджета Share. На цьому рекламному веб-сайті використовуються такі типи файлів cookie: «постійні файли cookie першої сторони» та «файли cookie сеансу».

«Основні постійні файли cookie» дозволяють відстежувати таку інформацію про відвідувачів нашого веб-сайту:

- IP-адреса (анонімна)
- Розташування: країна, регіон, місто, приблизна широта та довгота (геолокація)
- Дата і час звернення (відвідування сайту)
- Назва сторінки, що переглядається (Page Title)
- URL сторінки, що переглядається (URL сторінки)
- URL-адреса сторінки, яку переглядали до поточної сторінки (URL-адреса переходу)
- Роздільна здатність екрана пристрою користувача
- Час у часовому поясі місцевого відвідувача
- Файли, які були натиснуті та завантажені (Завантажити)
- Посилання на зовнішній домен, які були натиснуті (Outlink)
- Час генерації сторінок (час, потрібний веб-сторінкам, які генеруються веб-сервером і потім завантажуються відвідувачем: швидкість сторінки)
- Основна мова браузера, який використовується (заголовок Accept-Language)
- Версія браузера, плагіни браузера (PDF, Flash, Java, …), версія операційної системи, ідентифікатор пристрою (заголовок User-Agent)
- Мова відвіданої сторінки
- Кампанії
- Пошук на сайті

- Події

Зібрані дані не будуть передаватись жодним іншим організаціям для маркетингу, дослідження ринку чи комерційних цілей. Крім того, вищезазначені дані не можуть бути використані для ідентифікації конкретного відвідувача.

«Основні постійні файли cookie» створюються цим веб-сайтом і дозволяють:

- належне функціонування веб-сайту;
- збір статистики для покращення функціональності веб-сайту – для цього веб-сайт використовує Google Analytics (додаткову інформацію наведено нижче);
- функції обміну в соціальних мережах.
- Термін дії «постійних» файлів cookie закінчується через тринадцять місяців (13), після чого вони автоматично видаляються з пристрою користувачів. Файли cookie «технічної сесії» не містять жодних даних – вони розміщуються на час сеансу користувача (час, витрачений на перегляд веб-сайту).

Ці файли cookie необхідні для збереження вибору відвідувача під час доступу до веб-сайту. Коли відвідувач залишає веб-сайт, сеансовий файл cookie видаляється.

«Сторонні файли cookie» (включаючи файли cookie Google Analytics) описано нижче. «Сторонні файли cookie» з віджета «Поділитися» розміщуються на комп'ютері, якщо користувач погодився, щоб дозволити користувачам ділитися вмістом у соціальних мережах.

Веб-сайт не встановлює файли cookie з відображенням посилань на наші соціальні мережі, коли ви переглядаєте наш веб-сайт

ВІДХИЛЕННЯ

Коли веб-сайт відкривається вперше, відвідувач веб-сайту має вибір прийняти («ОК, я згоден») або відмовитися («Відхилити файли cookie») від розміщення файлів cookie.

Прийняти файли cookie: натиснувши цю опцію, відвідувач дає згоду на розміщення всіх файлів cookie для:

Оптимальна робота сайту

Функція обміну інформацією в соціальних мережах

Збірка статистики

Відхилити файли cookie: натискаючи цю опцію, відвідувач не дає згоди на розміщення будь-яких із зазначених вище файлів cookie. У цьому випадку розміщується лише сеансовий файл cookie; це технічний файл cookie, основна мета якого – запам’ятати вибір відвідувачів. Цей файл cookie розміщується на тривалість сеансу користувача (час, витрачений на перегляд веб-сайту) і автоматично видаляється, коли цей сеанс закінчиться. Вибір не приймати файли cookie не заважає вашій навігації веб-сайтом.

Вибір не зроблено: якщо відвідувач не приймає і не відмовляється від файлів cookie, веб-сайт розглядає це як відмову в розміщенні файлів cookie, і всі пов’язані функції призупиняються, доки не буде зроблено вибір.

Жодні файли cookie не розміщуються на пристроях відвідувачів, окрім випадків, коли було надано згоду, натиснувши опцію «ОК, я згоден».

ВІДМОВА

Якщо відвідувач погодився на розміщення файлів cookie, завжди можна змінити це рішення та відмовитися. Щоб відмовитися, відвідувачі повинні видалити всі файли cookie зі свого браузера. Однак якщо ви це зробите, вам,

можливо, доведеться вручну налаштовувати деякі параметри кожного разу, коли ви відвідуєте сайт, а деякі служби та функції можуть не працювати.

Щоб дізнатися, як очистити файли cookie в різних браузерах, відвідайте: https://www.aboutcookies.org/

ВАРІАНТ НЕ ВІДСЛІЖУВАТИ

Do Not Track — це технологія, яка дозволяє відвідувачам відмовитися від відстеження веб-сайтами з будь-якою метою, включаючи використання аналітичних служб, рекламних мереж і соціальних платформ. Ви можете ввімкнути опцію «Не відстежувати» безпосередньо у своєму веб-браузері. Google Analytics не відстежуватиме користувачів, які ввімкнули цю опцію у своїх веб-переглядачах.

GOOGLE ANALYTICS

Веб-сайт використовує Google Analytics для відстеження інформації відвідувачів, описаної вище. З цією метою вищезазначені зібрані дані передаються до Google Inc. Веб-сайт анонімізує IP-адреси відвідувачів перед їх передачею до Google Inc; це захищає анонімність відвідувачів, які вибрали повний функціонал веб-сайту. Google Analytics реалізував функцію контролю збереження даних. Ця функція надає власникам веб-сайтів можливість визначати період зберігання даних, що зберігаються в обліковому записі Google Analytics. Визначений термін зберігання становить 26 місяців; будь-які дані після закінчення цього періоду видаляються із серверів Google.

3. Особливості користування персональними даними, що були надані державним інституціям.

Доступ до персональних даних надається співробітникам Комісії, відповідальним за виконання цієї операції обробки, та іншим уповноваженим працівникам відповідно до принципу «необхідно знати». Такий персонал

дотримується статутних і, якщо потрібно, додаткових угод про конфіденційність. Для певної конкретної обробки доступ до персональних даних надається співробітникам EEAS на основі принципу «необхідно знати».

Персонал OLAF, IDOC, IAS (служби внутрішнього аудиту), Юридична служба Комісії, а також персонал інших генеральних директоратів (SG, DG BUDG і центр обміну інформацією) за запитом, необхідним у контексті офіційних розслідувань або з метою аудиту.

Згідно зі статтею 3(13) Регламенту (ЄС) 2018/1725 державні органи (наприклад, Рахункова палата, Суд ЄС), які можуть отримувати персональні дані в рамках конкретного запиту відповідно до законодавства Союзу або держави-члена, повинні не розглядаються як одержувачі. Подальша обробка цих даних цими державними органами повинна здійснюватися відповідно до застосовних правил захисту даних відповідно до цілей обробки.

Доступ до персональних даних надається співробітникам ЄСЗД у представництвах ЄС, відповідальним за виконання цієї операції обробки, та уповноваженому персоналу відповідно до принципу «необхідно знати». Такий персонал дотримується статутних і, якщо потрібно, додаткових угод про конфіденційність.

Доступ до персональних даних надається зовнішнім підрядникам, які працюють від імені та за договірною угодою з Контролером даних і беруть участь у створенні, підтримці, управлінні, архівуванні веб-сайтів та комунікаційній діяльності відповідно до принципу «необхідно знати» та з метою управління підписками на отримання інформації.

Обробка персональних даних підрядником і комунікаційними компаніями, яких уклали представництва ЄС від імені Комісії, може передбачати міжнародну передачу, якщо підрядники не є компаніями, що не є ЄС/ЄЕЗ, або використовують місцеві офіси в країні, де реалізується проект/програма. У контексті діяльності зовнішньої дії.

Ці перекази засновані на рішення про достатність – Імплементаційне рішення Комісії (ЄС) 2021/1772 від 28 червня 2021 року згідно з Регламентом

(ЄС) 2016/679 Європейського парламенту та Ради щодо належного захисту персональних даних Сполученим Королівством;

відступи, а саме з важливої причини суспільного інтересу (стаття 50(1)(d)).

Зібрана інформація не передаватиметься третім особам, за винятком випадків і з метою, яку ми можемо вимагати від нас згідно із законом.

4. Важливість захисту персональних даних у процесі електронного урядування.

Важливість захисту персональних даних у процесі електронного урядування в Європейському Союзі є важливою та актуальною темою. Оскільки ми є свідками зростаючої цифровізації державних процесів, забезпечення безпеки та конфіденційності особистих даних громадян має першочергове значення для підтримки громадської довіри та захисту основних прав.

Ось кілька ключових думок щодо важливості цієї теми:

Правова та нормативна база:

Дослідження має глибоко заглибитися в існуючу правову та нормативну базу, що регулює захист персональних даних у ЄС. Аналіз таких механізмів, як Загальний регламент захисту даних (GDPR), і розуміння того, як країни-члени впроваджують і адаптують ці правила до свого конкретного контексту електронного урядування, дадуть цінну інформацію.

Технологічні заходи:

Вивчення технологічних заходів, що застосовуються для захисту персональних даних, має вирішальне значення. Необхідно оцінити інтеграцію розширеного шифрування, безпечного зберігання даних і надійних механізмів автентифікації. Крім того, було б актуальним розуміння того, як такі нові технології, як блокчейн, можна використовувати для покращеного захисту даних в електронному урядуванні.

Виклики та можливості:

Досягнення балансу між потребою в ефективному електронному урядуванні та обов'язковим захистом конфіденційності особистих даних створює невід'ємні проблеми. Важливо визначити ці проблеми та запропонувати стратегії їх подолання. Крім того, не менш важливим є визнання можливостей для інновацій у захисті даних у сфері електронного урядування.

Сприйняття та довіра користувачів:

Дослідження має дослідити, як громадяни сприймають та довіряють системам електронного урядування щодо захисту їхніх персональних даних. Розуміння суспільного ставлення, занепокоєння та очікувань буде вкрай важливим для розробників політики та адміністраторів для розробки процесів електронного урядування, орієнтованих на користувача.

Порівняльний аналіз:

Враховуючи різноманітність країн-членів ЄС, проведення порівняльного аналізу їхніх практик електронного урядування має значну цінність. Визначення найкращих практик, загальних тенденцій і потенційних сфер для вдосконалення може надати практичну інформацію для розробників політики як на національному рівні, так і на рівні ЄС.

Практичні наслідки:

Дослідження має не лише сприяти академічним знанням, але й мати практичні наслідки для політиків, урядових органів і розробників технологій. Рекомендації щодо посилення захисту персональних даних у процесах електронного урядування мають бути чіткими, дієвими та враховувати технологічний ландшафт, що розвивається.

Таким чином, важливість захисту персональних даних у процесі електронного урядування в ЄС є складним і багатогранним питанням.

Комплексне вирішення потребує цілісного підходу, який враховує правові, технологічні, соціальні та етичні аспекти для створення міцної основи для безпечного та надійного електронного урядування.

Список використаних джерел:

1. PROTECTION OF YOUR PERSONAL DATA. *Moving forward together :* website. URL : https://eu4ukraine.eu/en/privacy-statement-en

2. Wahl, T. New Data Protection Framework for EU Institutions. *EUCRIM :* website. URL : https://eucrim.eu/news/new-data-protection-framework-eu-institutions/