ІНСТИТУЦІЙНТЙ ПРИМУС ЯК ІНСТРУМЕНТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1. Захист персональних даних, який здійснюється поліцією та органами кримінальної юстиції.
2. Захист даних у правоохоронних органах.
3. Юридична відповідальність за порушення законодавства про захист персональних даних.

1. Захист персональних даних, який здійснюється поліцією та органами кримінальної юстиції.

Директива (ЄС) 2016/680 – Захист осіб щодо обробки їхніх персональних даних поліцією та органами кримінального правосуддя та щодо вільного переміщення таких даних. Директива замінила Рамкове рішення 2008/977/JHA про захист персональних даних, що обробляються в рамках поліцейського та судового співробітництва у кримінальних справах, набувши чинності з 6 травня 2018 року.

ЯКА МЕТА ДИРЕКТИВИ?

Директива (ЄС) 2016/680, законодавча директива щодо захисту даних (LED), забезпечує захист персональних даних осіб, які беруть участь у кримінальному провадженні, будь то свідки, потерпілі або підозрювані.

Він встановлює всеосяжну структуру для забезпечення високого рівня захисту даних, враховуючи при цьому специфіку поліції та сфери кримінального правосуддя.

Він сприяє підвищенню довіри та полегшує співпрацю у боротьбі зі злочинністю в Європі шляхом гармонізації захисту персональних даних правоохоронними органами в країнах-членах Європейського Союзу (ЄС) та країнах Шенгенської угоди.

Директива є частиною реформи захисту даних ЄС разом із загальним регламентом захисту даних (GDPR) (див. резюме) та Регламентом (ЄС) 2018/1725 щодо захисту фізичних осіб щодо обробки персональних даних ЄС установи, органи, установи та установи (див. резюме).

КЛЮЧОВІ МОМЕНТИ

Директива вимагає, щоб дані, зібрані правоохоронними органами, були такими:

- обробляються законно та чесно;
- збираються для визначених, явних і законних цілей і обробляються лише у спосіб, сумісний із цими цілями;
- адекватні, відповідні та не надмірні щодо мети, з якою вони обробляються;
- точні та оновлені, де необхідно;
- зберігається у формі, яка дозволяє ідентифікувати особу не довше, ніж це необхідно для цілей обробки;
- належним чином захищені, включаючи захист від несанкціонованої або незаконної обробки, використовуючи відповідні технічні чи організаційні заходи.

Держави-члени повинні встановити часові обмеження для видалення персональних даних або регулярного перегляду необхідності зберігання таких даних.

Зацікавлені особи («суб'єкти даних»)

Директива вимагає від правоохоронних органів чітко розрізняти дані різних категорій осіб, зокрема:

- ті, щодо яких є серйозні підстави вважати, що вони вчинили або збираються вчинити кримінальне правопорушення;
- засуджені за вчинення кримінального правопорушення;
- жертви кримінальних правопорушень або ті, про кого є обґрунтовані припущення, що вони можуть бути жертвами кримінальних правопорушень;
- осіб, які є учасниками кримінального правопорушення, у тому числі потенційних свідків.

Особи мають право на те, щоб компетентні правоохоронні органи надали їм певну інформацію, а в деяких випадках її надали, зокрема:

- назву та контактні дані компетентного органу, який визначає мету та засоби обробки даних;
- цілі обробки їхніх даних;
- право подати скаргу до контролюючого органу та контактні дані органу;
- наявність права вимагати доступу та виправлення чи видалення своїх персональних даних, а також права обмежувати обробку своїх персональних даних.

Особи мають право отримати підтвердження від компетентних органів щодо того, чи обробляються їхні персональні дані, а також отримати доступ до таких даних та інформації, що стосується їх обробки.

Національні органи влади повинні вжити технічних та організаційних заходів для забезпечення рівня безпеки персональних даних, який відповідає ризику. Якщо обробка даних автоматизована, необхідно вжити ряд заходів, зокрема:

- недопущення сторонніх осіб до обладнання, яке використовується для обробки;

- запобігання несанкціонованому читанню, копіюванню, зміні або видаленню носіїв даних*;
- запобігання несанкціонованому введенню персональних даних і несанкціонованому перегляду, зміні або видаленню збережених персональних даних.

Національні органи влади повинні вести журнали з такою інформацією, як дата та час доступу до персональних даних та імена тих, хто переглядав ці дані або кому ці дані були розкриті. Журнали в основному використовуються для перевірки законності обробки, забезпечення безпеки та цілісності обробки та для кримінального провадження.

2. Захист даних у правоохоронних органах.

Специфічний характер поліцейської та судової діяльності у кримінальних справах означає, що в контексті такої діяльності потрібні різні правила щодо захисту персональних даних, щоб полегшити вільний потік даних та сприяти співпраці між державами-членами в цих сферах.

Директива про захист персональних даних, що обробляються з метою запобігання, розслідування, виявлення або переслідування кримінальних правопорушень, була прийнята в 2016 році та набула чинності в 2018 році.

Він спрямований на захист права осіб на захист їхніх персональних даних, гарантуючи при цьому високий рівень громадської безпеки.

Ця директива стосується як транскордонної, так і національної обробки даних компетентними органами держав-членів з метою:

- попередження, розслідування, розкриття та переслідування кримінальних правопорушень
- захист і запобігання загрозам громадській безпеці

Вона не охоплює діяльність інституцій, органів, офісів і агентств ЄС, а також діяльність, що виходить за межі законодавства ЄС.

Директива про захист персональних даних для запобігання, розслідування, виявлення або переслідування кримінальних правопорушень (Офіційний журнал ЄС)

Директива встановлює низку принципів, включаючи необхідність гарантувати, що будь-які зібрані персональні дані:

- обробляється законно
- збирається для конкретних, явних і законних цілей
- не є надмірним щодо мети, з якою він обробляється

Правила включають зобов’язання держав-членів надавати зрозумілу інформацію та забезпечувати права суб’єкта даних на доступ, виправлення, стирання та обмеження обробки. Однак вони також встановлюють обмеження на ці права, дозволяючи державам-членам приймати законодавчі заходи щодо їх обмеження.

Директива щодо захисту персональних даних, які обробляються з метою виконання кримінального законодавства, описує обов’язки контролерів даних (тих, хто відповідає за обробку даних). До них належать:

- призначення уповноваженого із захисту даних, щоб допомогти компетентним органам забезпечити дотримання правил захисту даних
- вимога щодо проведення оцінки впливу, якщо тип обробки може призвести до високого ризику для прав суб’єктів даних

Органи нагляду можуть бути такими ж, як ті, що встановлені згідно із загальним положенням про захист даних. Директива визначає правила про обов'язкову взаємодопомогу та загальне зобов'язання щодо співпраці.

Європейська консультативна рада із захисту даних забезпечує повне застосування цієї директиви. Ця рада складається з представників усіх 27 незалежних наглядових органів, а також контролює застосування GDPR.

Директива надає особам право на отримання компенсації, якщо вони зазнали шкоди внаслідок обробки, яка не відповідала правилам.

Передача персональних даних до країн, що не входять до ЄС, може відбуватися лише в тому випадку, якщо це вимагається для правоохоронних цілей і якщо Європейська комісія прийняла рішення щодо адекватності рівня захисту, який забезпечує відповідна країна.

Якщо немає рішення про достатність, передачі можуть відбуватися за наявності відповідних гарантій.

3. Юридична відповідальність за порушення законодавства про захист персональних даних.

Щоб забезпечити відповідність GDPR, важливо розуміти ролі контролерів і обробників даних. Саме вони збирають і обробляють особисті дані користувачів і, таким чином, відповідають за безпеку та конфіденційність даних на щоденному рівні.

Контролер даних відповідно до GDPR є «особою», але насправді, ймовірно, організацією, яка збирає персональні дані та визначає цілі та засоби їх обробки. Обробка даних може означати що завгодно: від створення профілів клієнтів до збору демографічної інформації для продажу.

Обробник даних — це особа — знову ж таки, швидше за все організація — яка обробляє персональні дані від імені контролера даних. Рекламні партнери – яскравий тому приклад. Вимоги GDPR стосуються як контролерів даних, так і обробників даних, але конкретні обов’язки відрізняються. Зрештою, відповідальність за безпеку даних і дотримання конфіденційності зазвичай несе контролер.

Контролери даних несуть основну відповідальність за забезпечення відповідності GDPR. Вони повинні отримати дійсну згоду фізичних осіб на обробку даних. (Див. ст. 7 GDPR щодо умов дійсної згоди.) Їхні додаткові обов’язки включають:

- ведення безпечних записів налаштувань згоди
- збереження точних і актуальних даних

- виправлення або видалення даних за запитом, за певних обставин
- впровадження відповідних технічних та організаційних заходів для захисту даних

Контролери даних також повинні переконатися, що будь-які сторонні обробники даних, з якими вони працюють, відповідають вимогам GDPR і мають договірні угоди.

Обробники даних повинні обробляти персональні дані лише відповідно до інструкцій та договірної угоди з контролером даних. До їх додаткових обов'язків входить:

- впровадження відповідних технічних та організаційних заходів для захисту даних
- повідомлення контролера даних про будь-які порушення даних
- ведення обліку діяльності з обробки
- дотримання вимог щодо видалення даних після обробки

Орган із захисту даних (DPA)

Органи захисту даних (DPA) є незалежними державними органами, які здійснюють нагляд за дотриманням та виконанням GDPR у кожній державі-члені ЄС. Як правило, кожна країна-член ЄС має власний DPA, який забезпечує дотримання GDPR та інших місцевих або регіональних законів про конфіденційність. DPA мають повноваження розслідувати порушення GDPR, накладати штрафи та наказувати організаціям вжити виправних заходів.

Хто зобов’язаний стежити за дотриманням GDPR?

Безумовно, DPA, але організаціям необхідно щодня контролювати обробку даних і безпеку. Це стосується того, які сторонні постачальники, як-от обробники даних та інші партнери, обробляють дані користувачів.

Крім того, технологічний і правовий ландшафти постійно змінюються, тому організаціям потрібно йти в ногу з цими змінами. Рішення для керування

згодою може допомогти автоматизувати та відповідати вимогам GDPR щодо отримання згоди на використання файлів cookie та трекерів, але це є основним обов'язком юрисконсульта та/або експерта з конфіденційності.

Поширені проблеми та виклики щодо відповідності GDPR

Забезпечення відповідності GDPR може бути складним завданням, особливо для малих і середніх організацій. У багатьох випадках відповідність GDPR вимагає призначення спеціаліста із захисту даних (DPO). У невеликих організаціях це може бути хтось, хто вже має іншу роботу в компанії.

Поширені проблеми з відповідністю включають:

- розуміння конкретних обов'язків організації щодо відповідності
- отримання дійсної згоди користувача
- налаштування та підтримка рішення для керування згодою
- впровадження відповідних заходів безпеки даних
- своєчасне виконання запитів щодо прав суб'єктів даних, особливо коли менша організація має обмежені ресурси
- повідомляти DPA про порушення даних протягом 72 годин

Найкращі практики для відповідності GDPR

Щоб увімкнути та підтримувати відповідність GDPR, організації повинні запровадити найкращі методи захисту даних і конфіденційності. Деякі з цих дій є нормативними вимогами в деяких країнах, але лише рекомендаціями щодо безпеки та відповідності в інших країнах. Важливо перевірити GDPR та інші місцеві норми щодо вимог, які застосовуються до вашого бізнесу:

- проведення аудитів даних для повного розуміння діяльності з обробки даних

- проведення оцінки впливу на захист даних
- впровадження політик і процедур захисту даних
- навчання співробітників щодо відповідності GDPR
- призначення кваліфікованого та добре поінформованого DPO (у деяких випадках не в компанії для доступу до достатнього досвіду)
- співпрацювати з перевіреними сторонніми постачальниками та постачальниками послуг, які відповідають GDPR
- використання комплексного рішення для керування згодою онлайн для збору та зберігання дійсної згоди користувача

Штрафи за недотримання GDPR

Застосування GDPR — це процес забезпечення відповідності організацій нормам GDPR, як-от отримання згоди перед обробкою даних. Це може включати такі дії, як розслідування звітів про порушення або перевірки обробки компанією даних користувачів, зокрема інформації про згоду. Організації, які не дотримуються вимог GDPR, можуть зіткнутися зі значними штрафами та іншими покараннями, незалежно від того, чи вдалося отримати дійсну згоду, зазнати порушення даних чи іншої проблеми.

Штрафи GDPR можуть становити до 20 мільйонів євро, або 4% річного глобального доходу компанії, залежно від того, що більше, за серйозні чи повторні порушення, або 10 мільйонів євро, або 2% річного глобального доходу компанії, залежно від того, що більше, за легші або перші злочини. DPA також може наказати тимчасово або назавжди припинити діяльність з обробки даних або навіть видалити дані.

Найбільший штраф GDPR на сьогоднішній день був накладений на американську компанію Meta, колишню Facebook, на 1,3 мільярда доларів США за обробку інформації користувачів. Регулятори конфіденційності ЄС дали компанії п’ять місяців, щоб припинити передачу даних користувачів із ЄС до Сполучених Штатів. З липня 2020 року ЄС і США не мають рамок ЄС-США

Privacy Shield, які охоплюють міжнародну передачу даних, коли її було визнано недійсною рішенням у справі «Шремс II».

Штрафні санкції означають нездатність контролерів даних і обробників належним чином дотримуватись GDPR через розуміння та забезпечення обробки своїх даних, неспроможність продемонструвати законне використання обраної ними правової основи та інші проблеми. Контролери та обробники даних також несуть відповідальність за «лікування» порушень GDPR, щоб гарантувати, що проблеми не виникатимуть і не повторюватимуться в майбутньому.

Однак, на відміну від деяких інших законів про конфіденційність даних, як-от у Сполучених Штатах, згідно з GDPR не існує «періоду виправлення», коли організації, звинувачені або визнані в порушенні закону, можуть виправити або виправити проблеми з конфіденційністю даних, не зазнаючи покарань.

Список використаних джерел:

1. Data protection in law enforcement. *European Council :* website. URL : https://www.consilium.europa.eu/en/policies/data-protection/data-protection-law-enforcement/
2. Protecting personal data that is used by police and criminal justice authorities (from 2018). *EUR-LEX :* website. URL : https://eur-lex.europa.eu/EN/legal-content/summary/protecting-personal-data-that-is-used-by-police-and-criminal-justice-authorities-from-2018.html
3. Who is responsible for GDPR compliance? *Usercentrics :* website. URL : https://usercentrics.com/knowledge-hub/who-is-responsible-for-gdpr-compliance/