Правила європейського права про захист персональних даних

1. Правила щодо законної обробки персональних даних.
2. Правила щодо безпеки обробки персональних даних.
3. Правила щодо підзвітності та сприяння відповідності персональних даних.

Правила щодо законної обробки персональних даних.

Розділ II Загального регламенту захисту персональних даних під назвою «Принципи» передбачає, що вся обробка персональних даних, по-перше, повинна здійснюватись з дотриманням принципів щодо якості даних, передбачених статтею 5 ЗРЗПД. Один із принципів передбачає, що персональні дані повинні «оброблятись законно, чесно та прозоро». По-друге, для того, щоб дані оброблялися законно, обробка має відповідати одній із законних підстав, які роблять обробку даних правомірною і які перераховані в статті 6341 для нечутливих даних та в статті 9 – для особливих категорій даних (або чутливих даних). Аналогічно розділ II Оновленої Конвенції 108, у якому йдеться про «основні принципи захисту персональних даних», визначає, що для того, щоб вважатися правомірною, обробка даних повинна бути «пропорційною до легітимної мети, яка переслідується».

Згода.

Щодо прав Ради Європи, у статті 5 (2) Оновленої Конвенції 108 зазначено положення щодо згоди. Вона також розглядається в практиці Європейського суду з прав людини (ЄСПЛ) та в декількох рекомендаціях Ради Європи. Щодо прав Європейського Союзу, згода як основа законної обробки персональних даних чітко визначена в статті 6 Загального

регламенту з питань захисту даних (ЗРЗПД), а також відображена в статті 8 Хартії основних прав ЄС. Ознаки чинної згоди роз'яснюються у визначенні згоди в статті 4, а умови отримання чинної згоди перераховані в статті 7, в той час як спеціальні правила для згоди дитини стосовно інформаційного суспільства встановлені в статті 8 ЗРЗПД. Згідно розділу 2.4, згода має бути надана добровільно, поінформовано, чітко визначено та однозначно. Згода повинна бути виражена у формі заяви або чіткої стверджувальної дії, якою дозволяється обробка даних, і особа має право відкликати її в будь-який час. Контролери зобов'язані зберігати записи про згоду для можливої перевірки.

Добровільна згода. Відповідно до положень Оновленої Конвенції 108 Ради Європи, згода суб'єкта даних має відображати вільне вираження наміреного вибору. Добровільна згода вважається чинною, якщо суб'єкт даних може зробити справжній вибір без ризику введення в оману, залякування, примусу чи значних негативних наслідків у разі відмови від згоди. Згідно законодавства Європейського Союзу, згода не є вільно наданою, якщо суб'єкт даних не має справжнього та вільного вибору або не може відмовитися чи відкликати згоду без негативних наслідків.

При оцінці добровільності згоди надання згоди на обробку даних, які не є обов'язковими для виконання договору чи надання послуг, має бути предметом особливої уваги. Суб'єкт персональних даних не повинен піддаватися прямому чи непрямому неналежному впливу, тиску або загрозам, щоб його згода рахувалася вільною. Якщо суб'єкт даних не може справжньо вибирати або не може відмовитися чи відкликати згоду без негативних наслідків, згода вважається не вільною.

Добровільна згода також може бути під сумнівом у випадках субординації, коли існує значний економічний або інший дисбаланс між контролером та суб'єктом даних, що надає згоду. Такий дисбаланс може виникнути, наприклад, в контексті трудових відносин, коли роботодавець обробляє персональні дані працівника. У таких випадках згода працівника

може бути сумнівною, оскільки він може не мати реального вибору через залежність від роботодавця та можливі негативні наслідки в разі відмови від згоди.

Приклад 1.

У випадку, коли деякі органи місцевого самоврядування вирішили виготовити електронні картки із вшитими чипами, що вказують місце проживання, і це стало обов'язковою умовою для отримання доступу до ряду важливих адміністративних послуг, таких як сплата місцевих податків онлайн, подання електронних скарг, купівля квитків для місцевих заходів тощо, обробка даних мешканців не може ґрунтуватися на згоді, оскільки в даному випадку існує необов'язковий, але опосередкований тиск на мешканців отримати ці електронні картки.

Відповідно до Загального регламенту з захисту персональних даних (ЗРЗПД), обробка персональних даних мешканців має базуватися на легітимних підставах. Органи місцевої влади можуть посилатися на статтю 6 (1)(e) ЗРЗПД, яка дозволяє обробку персональних даних, якщо це необхідно для виконання завдань, що виконуються у суспільних інтересах або у межах виконання офіційних повноважень, які покладені на контролера.

Однак важливо враховувати, що використання цієї підстави повинно бути обґрунтоване і відповідати принципам необхідності та пропорціональності. Органи місцевого самоврядування повинні докладати зусиль для забезпечення того, щоб обробка персональних даних відповідала принципам ЗРЗПД та не порушувала права і свободи мешканців.

Проінформована згода. Положення Загального регламенту з захисту персональних даних (ЗРЗПД) та Пояснювальна записка до Оновленої Конвенції 108 Ради Європи вказують на важливість поінформованої згоди, яка має бути надана фізичною особою перед тим, як вона виражає свою згоду на обробку її персональних даних.

Згідно з ЗРЗПД, поінформована згода повинна базуватися на ясній та зрозумілій інформації, яка надається суб'єкту даних. Фізичні особи повинні отримати точний та повний опис таких аспектів, як характер даних, які будуть оброблятися, цілі обробки, можливі одержувачі та права суб'єкта даних.

Пояснювальна записка до Оновленої Конвенції 108 також наголошує на важливості надання інформації про наслідки рішення суб'єкта даних, тобто про те, які факти призведе згода та обсяг, на який погоджується суб'єкт даних.

Згода повинна бути добровільною і надаватися вільним та свідомим чином. Суб'єкт даних повинен бути здатним зробити справжній вибір, не піддаючись ризику введення в оману, залякування, примусу або значних негативних наслідків у разі відмови від надання згоди.

Точно визначена згода. Так, Загальний регламент з захисту персональних даних (ЗРЗПД) визначає, що згода повинна бути точно визначеною відносно цілі обробки, і ця ціль повинна бути чітко описана в однозначних формулюваннях. Це важливий аспект забезпечення поінформованої та вільно наданої згоди від суб'єкта даних.

Якщо операції з обробки даних додаються або змінюються у спосіб, який не було розумно передбачити при наданні початкової згоди, то суб'єкта даних повинні повторно запитати про згоду. Це важливо з точки зору дотримання принципу цільової обмеженості та забезпечення того, щоб суб'єкти даних мали чітке розуміння того, для чого саме збираються обробляти їхні персональні дані. Якщо обробка має декілька цілей, то згода повинна надаватися щодо кожної з цих цілей. Це гарантує, що суб'єкти даних свідомі кожної конкретної мети обробки та можуть вільно висловити свою згоду для кожного конкретного використання їхніх персональних даних.

Однозначна згода. Згоду має бути надано однозначно. Це означає, що не може бути жодного розумного сумніву, що суб’єкт даних хотів висловити своє волевиявлення у вигляді дозволу на обробку своїх даних. Тож пасивність суб’єкта даних не свідчить про однозначну згоду. Наприклад, так буде у випадку, коли контролер отримує згоду суб’єкта даних, застосовуючи таку форму у своїх правилах конфіденційності: «використовуючи наш сервіс, ви надаєте згоду на обробку персональних даних». У такому випадку контролери мають пересвідчитися, що користувачі вручну та індивідуально погоджуються з такими правилами. Якщо згоду надано в письмовій формі, яка є частиною договору, згода на обробку персональних даних має бути індивідуалізована та у будь-якому випадку «мають існувати гарантії, що суб’єкт даних знає про факт надання згоди та її обсяг».

Необхідність виконання договору.

Так, відповідно до статті 6 (1)(b) Загального регламенту з захисту персональних даних (ЗРЗПД), обробка персональних даних є правомірною, якщо вона "необхідна для виконання договору, стороною якого є суб’єкт персональних даних, або для виконання заходів за вимогою суб’єкта даних до укладення договору". Це положення передбачає, що обробка персональних даних може мати правомірну підставу, якщо це є необхідним для виконання або укладення договору із суб'єктом даних. Це означає, що коли обробка персональних даних є необхідною для здійснення певних дій або укладання договору за вимогою суб'єкта даних, ця обробка є законною згідно із ЗРЗПД. Ця підстава для обробки даних визначається у випадках, коли існують конкретні відносини між сторонами, що передбачають укладання договору або виконання певних заходів на шляху до укладення договору.

Обробка особливих категорій даних.

Право РЄ залишає за національним законодавством можливість встановлення належного захисту для використання чутливих даних за умови дотримання статті 6 Оновленої Конвенції 108, а саме, що належні гарантії, вказані в інших положеннях Конвенції, встановлені законом. У праві ЄС стаття 9 ЗРЗПД містить детальні правила регулювання обробки особливих категорій даних (також названих «чутливими даними»).

Ці дані містять інформацію про расове або етнічне походження, політичні переконання, членство в профспілках, релігійні чи інші переконання, а також йдеться про обробку генетичних та біометричних даних для унікальної ідентифікації фізичної особи та дані про здоров'я, статеве життя або сексуальну орієнтацію. Обробка чутливих даних в принципі заборонена.

Проте у статті 9 (2) Регламенту можна знайти вичерпний перелік винятків із цієї заборони. Ці винятки становлять законні підстави для обробки чутливих даних:

• суб'єкт даних чітко і явно надав згоду на обробку даних;

• обробка здійснюється неприбутковою організацією з політичною, філософською, релігійною ціллю або для цілей професійної спілки в ході правомірної діяльності та за умови, що обробка стосується винятково членів чи колишніх членів організації або осіб, що в таких цілях регулярно підтримують контакт з нею;

• обробка стосується даних, які суб'єкт даних відкрито оприлюднив;

• обробка є необхідною:

• для здійснення обов'язків або реалізації спеціальних прав контролера або суб'єкта даних у трудовій сфері, у сфері соціальної безпеки та соціального захисту;

• для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи (коли суб'єкт даних не в змозі надати згоду);

• для формування, здійснення або захисту правових претензій або коли суди діють як судові органи;

•для цілей превентивної медицини чи гігієни праці: «для оцінювання працездатності працівника, медичного діагнозу, надання послуг у сфері охорони здоров'я чи соціального забезпечення чи лікування або управління системами та послугами в сфері охорони здоров'я чи соціального забезпечення чи лікування на підставі законодавства Союзу або держави-члена чи відповідно до договору з медичним працівником»;

• для цілей архівування в суспільних інтересах, для цілей наукових та історичних досліджень або статистичних цілей;

• з причин суспільного інтересу у сфері громадського здоров'я;

• з причин значного суспільного інтересу.

Життєво важливі інтереси суб'єкта даних або іншої особи. Відповідно до законодавства ЄС як і у випадку з нечутливими даними, життєво важливі інтереси суб'єкта даних або іншої особи можуть бути підставою для здійснення обробки чутливих даних. Така підстава для обробки чутливих даних, як життєво важливі інтереси суб'єкта даних або іншої особи, може бути законною підставою, якщо така обробка «не може очевидно ґрунтуватися на іншій правовій підставі». У деяких справах обробка персональних даних може захистити як індивідуальний, так і суспільний інтерес, наприклад, коли обробка необхідна в гуманітарних цілях. Для того, щоб обробка чутливих даних була легітимною на цій підставі, має бути відсутня можливість просити суб'єкта даних про згоду через те, що, наприклад, суб'єкт даних був без свідомості, або був відсутнім і з ним неможливо було зв'язатись. Інакше кажучи, особа була фізично або юридично нездатна надати згоду.

Благодійність або неприбуткові організації. Обробка персональних даних також дозволена в ході легітимної діяльності організацій, об'єднань або неприбуткових установ з політичною, світоглядною, релігійною ціллю або для цілей професійної спілки. Втім, обробка повинна стосуватися винятково членів, чи колишніх членів організації, чи осіб, що регулярно підтримують контакт з нею. Чутливі дані не можуть бути відкриті поза межами цих організацій за відсутності згоди суб'єкта даних.

Правила щодо безпеки обробки персональних даних.

Згідно як із законодавством Європейського Союзу, так із законодавством Ради Європи, контролери повинні дотримуватися загальної зобов'язаності прозорості та відповідальності під час обробки персональних даних, особливо у випадку витоку таких даних. У випадку порушення захисту персональних даних контролери повинні негайно повідомити орган контролю, за винятком ситуацій, коли ймовірність негайних ризиків для прав і свобод фізичних осіб є мала. Крім того, суб’єкти персональних даних мають бути проінформовані про витік таких даних, якщо існує значна ймовірність, що порушення може створити значний ризик для їхніх прав і свобод.

Відповідно до відповідних положень законодавства Європейського Союзу, контролери та оператори повинні, враховуючи сучасний рівень розвитку технологій, витрати на впровадження, а також характер, обсяг, контекст і цілі обробки персональних даних, а також ризики для прав і свобод фізичних осіб, вживати необхідні технічні та організаційні заходи для забезпечення відповідного рівня безпеки відповідно до зазначеного ризику.

Ці заходи, серед іншого, охоплюють:

• Застосування псевдонімів та шифрування персональних даних.

• Забезпечення конфіденційності, цілісності, доступності та стійкості систем та послуг з обробки.

• Своєчасне відновлення персональних даних і надання до них доступу у випадку технічної аварії.

• Реалізація процесу для систематичного тестування, оцінювання та аналізу ефективності технічних і організаційних заходів для гарантування безпеки обробки.

Часто існують індустріальні, національні та міжнародні стандарти, призначені для безпечної обробки даних. Наприклад, європейський Знак конфіденційності (EuroPriSe) є ініціативою проєкту "Транс'європейські

телекомунікаційні мережі" (eTEN) у складі Європейського Союзу, в рамках якого вивчаються можливості сертифікації продукції, зокрема програмного забезпечення, відповідно до європейських вимог щодо захисту персональних даних. Європейське агентство з мережевої та інформаційної безпеки (ENISA) було створене для зміцнення здатності Європейського Союзу, його членів та бізнес-спільноти в управлінні, запобіганні та реагуванні на проблеми мережевої та інформаційної безпеки. ENISA регулярно проводить.

Європейський Союз ухвалив Директиву про заходи для встановлення високого спільного рівня безпеки мережевих та інформаційних систем в межах Союзу (Директива MIC, NIS)443. Це перший узагальнений правовий інструмент ЄС у сфері кібербезпеки. Метою директиви є покращення кібербезпеки на національному рівні та підвищення рівня співпраці з Європейським Союзом. Вона також покладає на провайдерів ключових послуг (зокрема у галузях енергопостачання, охорони здоров'я, банківських послуг, транспорту, цифрової інфраструктури тощо) та провайдерів цифрових послуг відповідальність за управління ризиками, забезпечення безпеки їхніх мережевих та інформаційних систем, а також повідомлення про випадки порушення безпеки.

Згідно з законодавством Європейського Союзу (ЄС), Загальний регламент з питань захисту персональних даних (ЗРЗПД) визначає, що конфіденційність персональних даних є неотдільною частиною загального принципу. Постачальники публічно доступних послуг з електронної комунікації повинні гарантувати конфіденційність та забезпечувати безпеку своїх послуг. Згідно зі статтею 5 (1)(f), обробка персональних даних повинна гарантувати належну безпеку, включаючи захист від несанкціонованої або незаконної обробки, а також від випадкової втрати, знищення або пошкодження даних. Для досягнення цієї мети обов'язково використовувати належні технічні та організаційні заходи (принцип

"цілісності і конфіденційності"). Згідно зі статтею 32 контролер та оператор повинні застосовувати необхідні технічні та організаційні заходи для забезпечення високого рівня безпеки, такі як псевдонімізація, шифрування, регулярне тестування та відновлення даних у випадку технічної аварії.

Додатково, в статті 28 ЗРЗПД зазначено, що договір між контролером та оператором повинен містити положення, яке зобов'язує оператора забезпечити конфіденційність даних. Однак цей обов'язок не поширюється на ситуації, коли особа отримала дані як фізична особа, а не працівник контролера чи оператора, виключаючи випадки, які підпадають під виняток побутового характеру. Цей виняток не має застосовуватися до використання персональних даних в Інтернеті для необмеженої кількості користувачів чи обробки даних з професійним або комерційним характером.

Повідомлення про порушення захисту персональних даних.

Порушення захисту персональних даних означає невірне використання безпеки, що призводить до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних. Незважаючи на нові технології, такі як шифрування, які розширюють можливості забезпечення безпеки обробки, порушення захисту персональних даних залишається поширеним явищем. Причини таких порушень різноманітні, починаючи від ненавмисних помилок працівників організацій до зовнішніх загроз, таких як хакери та кіберзлочинці. Наслідки порушень захисту даних можуть бути серйозними для приватного життя та прав осіб, оскільки такі порушення призводять до втрати контролю над персональними даними. Можливі наслідки включають крадіжку, фінансові втрати, втрату конфіденційності, а також шкоду репутації.

Відповідно до ЗРЗПД і Оновленої Конвенції 108, контролери зобов'язані повідомляти компетентні органи про порушення захисту даних, які можуть спричинити серйозне втручання в права суб'єктів даних. Таке повідомлення повинно бути здійснене "без затримок" та містити докладний опис порушення, кількості потенційно затронутих суб'єктів даних, наслідків порушення та заходів, призначених для мінімізації цих наслідків. Якщо існує високий рівень ризику для прав і свобод суб'єктів даних, контролер повинен також повідомити їх про порушення. Винятки з цього обов'язку можуть бути застосовані, якщо контролер вже вжив відповідних заходів захисту даних, таких як шифрування, і якщо ці заходи дозволяють уникнути шкоди для суб'єктів даних.

Обов'язок повідомлення про порушення захисту даних покладається на контролера. Незалежно від того, чи здійснює обробку контролер чи оператор, важливо, щоб і оператори також були зобов'язані повідомляти про порушення. У випадку порушення захисту даних, оператори мають повідомити контролера про це негайно. Подальше відповідальне за повідомлення контролюючому органу та суб'єктам даних, яких стосується порушення, лежить на контролері. Це повідомлення повинно бути здійснене відповідно до правил і у відповідні строки, передбачені відповідними нормами.

Правила щодо підзвітності та сприяння відповідності персональних даних.

У Європі принцип підзвітності допомагає гарантувати дотримання правил захисту персональних даних. Контролери, тобто організації, які збирають і обробляють персональні дані, несуть відповідальність за дотримання цих правил. Вони повинні бути готові довести, що

дотримуються правил, навіть якщо порушення не відбулося. Для цього контролери повинні розробити і впровадити політику управління даними, яка включає технічні та організаційні заходи. Ці заходи, зокрема, передбачають призначення спеціаліста з питань захисту персональних даних, ведення записів і документації про обробку даних, а також здійснення оцінки впливу на приватне життя.

Документування обробки даних. Компанії часто повинні документувати свої дії, щоб показати, що вони дотримуються правил. Наприклад, податківці вимагають від компаній вести велику кількість документів. У сфері захисту персональних даних ведення записів також є важливим, оскільки це допомагає компаніям дотримуватися правил. Законодавство ЄС вимагає від контролерів вести записи про обробку персональних даних. Цей обов’язок гарантує, що контролюючі органи матимуть всю необхідну документацію для перевірки законності обробки.

Компанії, які обробляють персональні дані, повинні документувати наступну інформацію: 1) Ім'я та контактні дані компанії, яка обробляє дані, а також інших осіб, які можуть бути відповідальними за обробку, наприклад, співконтролера, представника контролера та відповідальної особи з питань захисту персональних даних; 2) Мети обробки персональних даних; 3) Категорії суб'єктів даних, дані яких обробляються, та категорії персональних даних, які обробляються; 4) Категорії отримувачів, яким можуть бути передані персональні дані;5) Чи були або будуть персональні дані передані третім державам або міжнародним організаціям; 6) Якщо можливо, строки, через які різні категорії персональних даних будуть видалені; 7) Огляд технічних заходів, які були впроваджені для забезпечення безпеки обробки.

Обов’язок вести записи про обробку персональних даних поширюється не лише на контролерів, а й на операторів. Це важливе нововведення, оскільки раніше обов’язки операторів визначалися в

основному в договорах між контролерами та операторами. Тепер цей обов’язок закріплений у законодавстві.

ЗРЗПД передбачає винятки з цього обов’язку. Наприклад, записи не потрібно вести, якщо в організації працює менше 250 осіб, якщо обробка не є систематичною, не стосується особливих категорій даних (наприклад, даних про здоров’я або релігію) або даних про засудження за злочини.

Записи про обробку персональних даних допомагають контролерам та операторам продемонструвати, що вони дотримуються правил захисту даних. Вони також дають можливість контролюючим органам перевіряти законність обробки. Якщо контролер або оператор отримує запит від контролюючого органу про надання доступу до записів, вони зобов’язані надати цей доступ.

Кодекс поведінки. Кодекс поведінки - це добровільний документ, який розробляється організацією або групою організацій для визначення стандартів обробки персональних даних у певній галузі. Кодекси поведінки можуть бути корисними для контролерів та операторів персональних даних, оскільки вони можуть допомогти їм:

Розуміти та дотримуватися вимог законодавства ЄС про захист персональних даних

Полегшити дотримання вимог законодавства

Покращити прозорість своїх практик обробки даних

Підвищити довіру суб'єктів даних

Законодавство ЄС про захист персональних даних (ЗРЗПД) закликає держави-члени, контрольні органи, Комісію та Європейську раду з захисту персональних даних заохочувати створення кодексів поведінки. ЗРЗПД також вимагає, щоб кодекси поведінки, які стосуються обробки в декількох державах-членах, були погоджені компетентним контролюючим органом і Європейською радою з захисту персональних даних.

Розробка кодексу поведінки починається з формування групи розробників. Група розробників складається з представників організацій, які будуть дотримуватися кодексу. Група розробників визначає цілі кодексу, його сферу застосування та конкретні положення.

Після завершення розробки кодексу він подається на погодження компетентному контролюючому органу. Контрольний орган проводить оцінку кодексу, щоб визначити, чи відповідає він вимогам ЗРЗПД. Якщо контрольний орган погоджує кодекс, він публікує його на своєму веб-сайті.

Комісія може вирішити, що погоджений кодекс поведінки матиме загальну чинність у межах Союзу. Це означає, що організації з усіх держав-членів ЄС зможуть дотримуватися кодексу, не отримуючи окремого погодження від контролюючого органу.

Вплив кодексів поведінки на захист персональних даних. Кодекс поведінки може мати значний вплив на захист персональних даних. По-перше, кодекси можуть допомогти організаціям зрозуміти та дотримуватися вимог законодавства ЄС про захист персональних даних. Це може допомогти запобігти порушенням законодавства та захистити права суб'єктів даних.

По-друге, кодекси можуть полегшити дотримання вимог законодавства. Це може бути особливо корисно для малих та середніх підприємств (МСП), які можуть не мати ресурсів, необхідних для самостійного дотримання законодавства.

По-третє, кодекси можуть покращити прозорість практик обробки даних. Це може допомогти суб'єктам даних зрозуміти, як їхні дані збираються та використовуються.

По-четверте, кодекси можуть підвищити довіру суб'єктів даних. Це може бути особливо важливо для організацій, які обробляють чутливі дані.

Кодекс поведінки може бути цінним інструментом для контролерів та операторів персональних даних. Кодекси можуть допомогти організаціям

дотримуватися вимог законодавства ЄС про захист персональних даних, полегшити дотримання вимог законодавства, покращити прозорість практик обробки даних та підвищити довіру суб'єктів даних.

Іншими засобами на додаток до кодексів поведінки, за допомогою яких контролери та оператори можуть продемонструвати дотримання ЗРЗПД, є механізм сертифікації, відзнаки та оцінки.

Механізм сертифікації - це добровільна система, яка дозволяє організаціям отримати сертифікат, що підтверджує їхнє дотримання вимог ЗРЗПД. Сертифікацію проводять незалежні органи, які мають відповідну кваліфікацію та досвід. Сертифікація може бути корисною для контролерів та операторів персональних даних, оскільки вона може:

Полегшити дотримання вимог ЗРЗПД

Підвищити довіру суб'єктів даних

Надати конкурентні переваги

Процес сертифікації починається з подання заявки на сертифікацію до органу сертифікації. Орган сертифікації проводить оцінку організації, щоб визначити, чи відповідає вона вимогам ЗРЗПД. Якщо організація відповідає вимогам, вона отримує сертифікат. Сертифікат має строк дії, який зазвичай становить один або три роки. Орган сертифікації проводить періодичні аудити, щоб переконатися, що організація продовжує відповідати вимогам ЗРЗПД.

Відзнаки та оцінки - це інші добровільні інструменти, які можуть використовуватися для демонстрації відповідності ЗРЗПД. Відзнаки зазвичай присуджуються організаціям, які досягли високих стандартів захисту персональних даних. Оцінки проводяться незалежними органами, які оцінюють конкретні аспекти діяльності організації. Відзнаки та оцінки можуть бути корисними для контролерів та операторів персональних даних, оскільки вони можуть:

Підвищити довіру суб'єктів даних

Надати конкурентні переваги

Процес присудження відзнаки або проведення оцінки починається з подання заявки до відповідного органу. Орган проводить оцінку організації, щоб визначити, чи відповідає вона критеріям відзнаки або оцінки. Якщо організація відповідає критеріям, їй присуджується відзнака або проводиться оцінка.

Механізм сертифікації, відзнаки та оцінки можуть мати позитивний вплив на захист персональних даних. Вони можуть допомогти організаціям зрозуміти та дотримуватися вимог ЗРЗПД, полегшити дотримання вимог законодавства та підвищити довіру суб'єктів даних. Однак, важливо зазначити, що ці інструменти не є обов'язковими. Організації не зобов'язані проходити сертифікацію, отримувати відзнаки або проходити оцінки. Деякі організації можуть вважати, що ці інструменти є надмірними або дорогими. Інші організації можуть вважати, що вони можуть забезпечити достатній захист персональних даних без цих інструментів.

У кінцевому рахунку, рішення про те, чи проходити сертифікацію, отримувати відзнаки або проходити оцінки, залишається за кожною організацією.

Механізм сертифікації, відзнаки та оцінки можуть бути особливо корисними для малих та середніх підприємств (МСП). МСП можуть не мати ресурсів, необхідних для самостійного дотримання вимог ЗРЗПД. Сертифікація, відзнаки та оцінки можуть допомогти МСП продемонструвати дотримання вимог ЗРЗПД та підвищити довіру суб'єктів даних. Організації, які розглядають можливість проходження сертифікації, отримання відзнаки або проходження оцінки, повинні провести дослідження, щоб визначити, який інструмент є найкращим для них. Вони повинні враховувати такі фактори, як:

Види діяльності організації

Розмір організації

Бюджет організації

Організації також повинні переконатися, що орган, який надає сертифікацію, відзнаку або оцінку, є авторитетним і має досвід роботи в галузі захисту персональних даних. Організації, які пройшли сертифікацію, отримали відзнаку або пройшли оцінку, повинні підтримувати свій статус шляхом дотримання вимог ЗРЗПД та періодичних аудитів.

Література.

Пояснювальна записка до Оновленої Конвенції 108, п.. 46; Рада Європи, Комітет міністрів (2010), Рекомендація Комітету міністрів CM/Rec(2010)13 державам-членам про захист осіб стосовно автоматичної обробки персональних даних у контексті профайлінгу, від 23 листопада 2010 р., стаття 3.4 (b).

Рішення Суду ЄС, C-536/15, «“Tele2 (Netherlands) BV” та інші проти Управління споживачів та ринку (УСР)» (Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)), від 15 березня 2017 р., п. 36.

Директива 2009/136/ЕС Європейського Парламенту та Ради від 25 листопада 2009 р., яка доповнює Директиву 2002/22/ЕС «Про універсальні послуги та права користувачів стосовно електронних мереж зв’язку та послуг, Директива 2002/58/ЕС «Про обробку персональних даних та захист таємниці у секторі електронних комунікацій» та Регламент (ЄС) № 2006/2004 «Про співробітництво між національними органами

влади, відповідальними за дотримання законів про захист прав споживачів», OJ 2009 L 337, с. 11.

Рішення Суду ЄС, C-543/09, «“Deutsche Telekom” проти Федеративної Республіки Німеччини» (Deutsche Telekom AG v. Bundesrepublik Deutschland), від 5 травня 2011 р.; п. 61.

Регламент (ЄС) № 526/2013 Європейського Парламенту та Ради від 21 травня 2013 р. щодо Європейського агентства з мережевої та інформаційної безпеки (ENISA) та про скасування Регламенту (ЄС) № 460/2004, OJ 2013 L 165.

Директива про конфіденційність та електронні комунікації, стаття 5 (1).

М. Бем, І. Городський. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. – «К.І.С.»., 2021. С. 161.