ПОРЯДОК ОРГАНІЗАЦІЇ ПРОЦЕСУ ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1. Система управління захистом даних
2. Політика приватності.
3. Обов’язки та відповідальність контролера, оператора щодо захисту персональних даних

1. Система управління захистом даних.

Система управління захистом даних (DPMS) — це основа, яка дозволяє компаніям розробляти та створювати ефективну інфраструктуру захисту даних. Він забезпечує їх систематичними правилами та положеннями, що охоплюють політику, процеси та дії, пов’язані з обробкою персональних даних. DPMS має рекомендації щодо визначення ролей і обов’язків людей у компанії, пов’язаних із захистом даних. Ефективне впровадження DPMS допомагає організаціям демонструвати дотримання вимог щодо захисту даних, підтримувати довіру та зміцнювати довірливі стосунки із зацікавленими сторонами, клієнтами та партнерами.

«Впровадження DMPS має починатися з огляду поточних і пов’язаних процесів, потім зачеплених і відповідальних осіб і завершуватися визначенням політики», – стверджує наш партнер expertree consulting.

З якими 2 труднощами стикаються під час управління захистом даних? Розсіяність даних, відсутність консолідованих систем, розосереджені дані та ручна робота – ось деякі з проблем, які компаніям потрібно знайти рішення. Програмне забезпечення для керування захистом даних є ключем до вирішення цих проблем і дозволяє організаціям налаштувати ефективне та робоче керування захистом даних.

Щоб запровадити DPMS, організації повинні почати з огляду поточних і пов’язаних процесів у компанії.

Життєвий цикл даних починається зі збору персональних даних до архівування/утилізації персональних даних) і проходить через їхні бізнес-процеси, системи, продукти чи послуги. Крім того, компанії повинні постійно контролювати та переглядати впровадження своїх політик захисту даних у процеси в масштабах організації.

Ось коротка інструкція щодо підтримки всіх процесів у DPMS:

1. Документуйте потоки персональних даних

Використовуйте карту інвентаризації даних або діаграму потоку даних.

Створіть реєстр згод.

2. Включіть захист даних у бізнес-процеси, системи, продукти чи послуги

Використовуйте підхід DPIA до захисту даних за проектом для систем або процесів, які є новими або зазнають серйозних змін.

Забезпечте дотримання політики захисту даних організації.

Використовуйте договірні положення

Проводити перевірки дотримання положень. Встановлювати процес для витоку даних.

Використовуйте журнал реєстрації інцидентів, щоб документувати інциденти та реагування після порушення.

3. *Налагодити моніторинг ризиків і звітність*

Управління ризиками за допомогою корпоративної системи управління ризиками з механізмами звітності.

Проводьте внутрішні аудити для моніторингу та оцінки реалізації політик і процесів захисту даних.

Вище керівництво має призначити принаймні одну особу на посаду спеціаліста із захисту даних (DPO), відповідального за всі питання, пов’язані

із захистом персональних даних і забезпечення дотримання конфіденційності даних.

Основні обов'язки DPO:

Забезпечує відповідність через політики та процеси захисту даних;

Сприяє розвитку культури захисту персональних даних і інформує зацікавлених сторін про політику захисту персональних даних;

Обробляє запити на доступ і виправлення персональних даних;

Керує запитами та скаргами щодо захисту персональних даних;

Попереджає керівництво про будь-які ризики, які можуть виникнути щодо персональних даних, які обробляє організація.

Політика захисту даних

Це невід’ємна частина корпоративного управління та має забезпечувати стратегічне керівництво щодо впровадження системи захисту даних.

Що має містити DPP:

Моніторинг та управління ризиками захисту персональних даних як частина корпоративної діяльності

управління

Ведення оцінки впливу на захист даних (DPIA)

Призначення DPO, CISO

Встановлення навчання співробітників із захисту даних

Виділення ресурсів для захисту даних, тобто бюджету та робочої сили

Надання інструкцій щодо управління витоками даних, реалізації планів виправлення та розгляду основних скарг.

2. **Політика приватності.**

Правила ЄС щодо захисту даних гарантують захист ваших особистих даних, коли вони збираються, наприклад, коли ви купуєте щось в Інтернеті, подаєте заявку на роботу чи просите кредит у банку. Ці правила застосовуються як до компаній і організацій (державних і приватних) у ЄС, так і до тих, що розташовані за межами ЄС, які пропонують товари чи послуги в ЄС, наприклад Facebook або Amazon, щоразу, коли ці компанії запитують або повторно використовують персональні дані окремих осіб. в ЄС.

Немає значення, який формат мають дані – онлайн у комп'ютерній системі чи на папері у структурованому файлі – щоразу, коли інформація, яка прямо чи опосередковано ідентифікує вас як особу, зберігається чи обробляється, ваші права на захист даних повинні поважатися.

Коли дозволена обробка даних?

Правила ЄС щодо захисту даних, також відомі як Загальний регламент ЄС щодо захисту даних (або GDPR), описують різні ситуації, коли компанії чи організації дозволяється збирати або повторно використовувати вашу особисту інформацію:

вони мають з вами договір – наприклад, контракт на постачання товарів чи послуг (тобто, коли ви купуєте щось онлайн) або трудовий контракт

вони дотримуються юридичних зобов'язань – наприклад, коли обробка ваших даних є вимогою законодавства, наприклад, коли ваш роботодавець надає інформацію про вашу місячну зарплату органу соціального захисту, щоб ви мали соціальне страхування

коли обробка даних відповідає вашим життєво важливим інтересам, наприклад, коли це може захистити ваше життя

для виконання публічного завдання – переважно пов'язаного із завданнями державних адміністрацій, таких як школи, лікарні та муніципалітети

якщо є законні інтереси – наприклад, якщо ваш банк використовує ваші особисті дані, щоб перевірити, чи маєте ви право на ощадний рахунок із вищою процентною ставкою

У всіх інших ситуаціях компанія або організація повинна запитати вашу згоду (відому як «згода»), перш ніж вони зможуть збирати або повторно використовувати ваші особисті дані.

Немає згоди, немає обробки даних

Коли компанія чи організація запитує вашу згоду, ви повинні виконати чітку дію, погоджуючись на це, наприклад, підписавши форму згоди або вибравши «так» із чіткого варіанту «так/ні» на веб-сторінці.

Недостатньо просто відмовитися, наприклад, встановивши прапорець, що ви не хочете отримувати маркетингові електронні листи. Ви повинні погодитися на збереження та/або повторне використання ваших особистих даних для цієї мети.

Вам також слід надати наступну інформацію, перш ніж ви вирішите підключитися:

інформацію про компанію/організацію, яка оброблятиме ваші дані, включно з їхніми контактними даними та контактними даними спеціаліста із захисту даних (DPO), якщо такий є

причина, чому компанія/організація використовуватиме ваші персональні дані

як довго вони збираються зберігати ваші персональні дані

відомості про будь-яку іншу компанію чи організацію, яка отримає ваші персональні дані

інформація про ваші права на захист даних (доступ, виправлення, видалення, скарга, відкликання згоди)

Вся ця інформація має бути представлена чітко та зрозуміло.

Відкликання згоди на використання персональних даних і права на заперечення

Якщо ви раніше дали згоду компанії чи організації на використання ваших персональних даних, ви можете зв'язатися з контролером даних (особою чи органом, який обробляє ваші персональні дані) і відкликати свій дозвіл у будь-який час. Після відкликання дозволу компанія або організація більше не зможе використовувати ваші особисті дані.

Якщо організація обробляє ваші персональні дані на основі власних законних інтересів або як частину завдання в суспільних інтересах чи для офіційної влади, ви можете мати право заперечити. У деяких конкретних випадках громадський інтерес може переважати, і компанії чи організації може бути дозволено продовжувати використовувати ваші особисті дані. Наприклад, це може стосуватися наукових досліджень і статистики, завдання, яке виконується як частина офіційної ролі державного органу.

Для електронних листів прямого маркетингу, які рекламують певні бренди чи продукти, потрібна ваша попередня згода. Однак, якщо ви вже є клієнтом певної компанії, вони можуть надсилати вам прямі маркетингові електронні листи про власні схожі продукти чи послуги. Ви маєте право в будь-який час відмовитися від отримання такого прямого маркетингу, і компанія повинна негайно припинити використання ваших даних.

У будь-якому випадку вам завжди слід надавати інформацію про право заперечувати проти використання ваших особистих даних, коли компанія чи організація вперше звертається до вас**.**

3. **Обов'язки та відповідальність контролера, оператора щодо захисту персональних даних**

У сучасному цифровому світі збір і зберігання даних є радше нормою, ніж винятком. Компанії можуть збирати індивідуальні дані для рекламних, маркетингових, аналітичних або дослідницьких цілей. Кожного разу, коли компанія збирає та обробляє персональні дані фізичної особи, вона робить це

як «контролер» або «обробник». У розділі 1, статті 4 GDPR, ці два визначення визначені нижче:

«Контролер» — це «фізична або юридична особа, державний орган, агентство чи інший орган, який самостійно або спільно з іншими визначає цілі та засоби обробки персональних даних».

Обробник стосується «фізичної або юридичної особи, державного органу, агентства чи іншого органу, який обробляє персональні дані від імені контролера».

Якщо організація контролює та несе відповідальність за особисті дані, які вона зберігає, вона є контролером даних. З іншого боку, якщо він зберігає персональні дані, але якась інша організація приймає рішення та несе відповідальність за те, що відбувається з даними, тоді це обробник даних

Згідно з чинною Директивою про захист даних 95/46/EC, лише контролери несуть відповідальність за недотримання вимог щодо захисту даних. Однак Загальний регламент ЄС із захисту даних (GDPR) досягне балансу, покладаючи прямі зобов'язання також на обробників даних.

Згідно зі статтею 83, у разі невідповідності штрафи можуть бути застосовані як до контролерів, так і до процесорів. Ці штрафи накладаються залежно від «ступеню відповідальності контролера або процесора з урахуванням технічних та організаційних заходів, які вони впроваджують».

Це суттєва зміна та різко збільшить профіль ризику для таких суб'єктів, як хмара та постачальники центрів обробки даних, які діють як процесори даних. Однак вплив також відчують контролери, які залучають їхні послуги, оскільки збільшення вартості відповідності може призвести до подальшого збільшення вартості послуг процесорів. Контролери також повинні бути особливо пильними щодо процесорів, з якими вони співпрацюють, і переконатися, що вони мають технічні та операційні заходи, необхідні для відповідності GDPR.

Тепер, коли ми визначили, що контролер і обробник поділять зобов'язання щодо захисту даних, давайте глибше розглянемо їхні обов'язки.

Контролер даних є основною стороною, яка відповідає за збір даних. Ці обов'язки контролера включають збір згоди осіб, зберігання даних, керування згодою-відкликанням, надання права доступу тощо. Крім того, він повинен мати можливість продемонструвати дотримання принципів, пов'язаних з обробкою персональних даних. Ці принципи перераховані в GDPR як «законність, справедливість і прозорість, мінімізація даних, точність, обмеження зберігання та цілісність, а також конфіденційність персональних даних».

GDPR надає додаткові відомості про те, як організації можуть продемонструвати, що їх діяльність з обробки є законною.

Якщо особа відкликає згоду, контролер несе відповідальність за ініціювання цього запиту. Тому після отримання цього запиту потрібно буде попросити обробника видалити відкликані дані з їхніх серверів.

Якщо кілька організацій поділяють відповідальність контролерів за обробку персональних даних, GDPR ЄС передбачає наявність спільних контролерів. Очікується, що спільний контролер за угодою визначає свої відповідні обов'язки контролера та надає зміст цієї угоди суб'єктам даних, визначаючи засоби зв'язку з обробниками з єдиною контактною точкою. Таким чином, GDPR покладає повну відповідальність на спільних контролерів.

Чинна Директива звільняє контролерів від відповідальності за шкоду, що виникає у випадках форс-мажорних обставин або непередбачуваних обставин, які перешкоджають їм виконати свою договірну угоду. Однак GDPR не містить такого винятку, тобто контролери можуть нести ризик у випадках форс-мажорних обставин.

Контролер повинен буде фіксувати всі порушення даних. Крім того, вони повинні на вимогу повідомляти про будь-які порушення даних органам із забезпечення дотримання GDPR. Оскільки 72-годинний термін для повідомлення про витоки даних, ймовірно, виявиться надзвичайно складним

для контролера даних, експерти радять організаціям призначити особу, яка буде брати на себе відповідальність за перевірку та повідомлення про витоки даних, а також запровадити чітку політику та процедури звітування про витоки даних, якщо це необхідно.

Очікується, що контролер працюватиме лише з процесорами з відповідними технічними та організаційними заходами для дотримання вказівок GDPR. Іншими словами, контролери даних, тобто клієнти обробників даних GDPR, повинні вибирати лише обробників, які відповідають GDPR, або самі ризикують отримати штрафні санкції.

Оскільки наглядові органи застосовують штрафи до контролерів за відсутність належної перевірки, обробники можуть виявитися зобов'язаними отримати незалежні сертифікати відповідності, щоб заспокоїти контролерів, які бажають скористатися їхніми послугами. Їм також може знадобитися вжити заходів для захисту даних, таких як шифрування та псевдонімізація, стабільність і безвідмовна робота, резервне копіювання та аварійне відновлення, а також регулярне тестування безпеки. Однак обробники за межами ЄС можуть чинити опір накладенню цих нових зобов'язань, що потенційно ускладнить контролерам законне призначення бажаних обробників, що призведе до більш складних переговорів щодо угод про аутсорсинг

Обробнику забороняється використовувати персональні дані, які йому довірено, для цілей, відмінних від тих, які визначені контролером даних. За запитом процесор повинен видалити або повернути всі персональні дані контролеру після закінчення контракту на надання послуг.

Він може передавати персональні дані в третю країну лише після отримання законного дозволу.

Він повинен отримати письмовий дозвіл від контролера, перш ніж залучати субпідрядника, і нести повну відповідальність за невиконання субпідрядниками вимог GDPR.

Обробник повинен увімкнути та сприяти аудиту відповідності, який проводить контролер або представник контролера.

У разі порушення даних обробник повинен повідомити контролерів даних без зайвої затримки

Крім того, обробник зобов'язаний вести облік діяльності з обробки даних, якщо він відповідає будь-якому з наступних критеріїв:

Працевлаштовано 250 і більше осіб

Обробляє дані, які «ймовірно призведуть до ризику для прав і свобод суб'єктів даних».

Обробляє дані частіше, ніж час від часу.

Обробляє спеціальні категорії даних, як зазначено в статті 9(1)

Обробляє дані, що стосуються кримінальних судимостей

Обробники також повинні будуть переглянути існуючі угоди про обробку даних, щоб переконатися, що вони виконали свої зобов'язання щодо дотримання вимог GDPR.

Обов'язки обробника даних відповідно до GDPR

Обов'язки обробника даних визначаються насамперед контролером, але можуть включати такі завдання, як збір даних, запис, організація, структурування, зберігання, зміна, пошук, консультації, використання, розкриття шляхом передачі, розповсюдження або іншим чином надання доступу, узгодження або поєднання, обмеження , стирання або знищення. Ці обов'язки мають бути визначені в підписаній угоді між Контролером і Обробником.

GDPR зобов'язує обробників вести облік своєї діяльності з обробки та вживати відповідних заходів безпеки. Крім того, обробники зобов'язані призначити спеціаліста із захисту даних (DPO), якщо вони здійснюють масштабну обробку спеціальних категорій даних. Якщо відбувається порушення даних, обробник зобов'язаний повідомити контролера без зайвої затримки.

Обов'язки контролера відповідно до GDPR

Контролер GDPR вирішує, чому персональні дані потрібно обробляти та як вони оброблятимуться. Як контролер відповідно до GDPR, організація повинна гарантувати, що всі дії з обробки даних відповідають принципам GDPR. Ці принципи включають законність, справедливість, прозорість, обмеження цілей, мінімізацію даних, точність, обмеження зберігання, а також цілісність і конфіденційність.

Контролери GDPR повинні продемонструвати відповідність цим принципам і можуть нести відповідальність за будь-які порушення. Щоб підтвердити відповідність, контролери повинні вести облік своєї діяльності з обробки, проводити оцінку впливу на захист даних для високоризикованої діяльності з обробки та забезпечувати впровадження належних заходів безпеки.

Підсумовуючи, ключова відмінність між GDPR контролера та контролером процесора полягає в тому, що контролер GDPR несе відповідальність за забезпечення загальної відповідності законам про захист даних, тоді як процесор діє за вказівками контролера.

Важливо пам'ятати, що хоча їхні обов'язки відрізняються, контролер даних і обробник повинні працювати разом, щоб забезпечити відповідність GDPR. Чітка комунікація та визначені ролі можуть допомогти кожній стороні ефективно виконувати свої зобов'язання.

Список використаних джерел:

1. Data protection and online privacy. *YOUR EUROPE* : website. URL : https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm

2. Data Protection Management System: Where to Start from. *Compliance-Aspekte* : website. URL : https://utilitiesone.com/telecommunications-and-personal-privacy-navigating-the-challenges

3. Monpi Neog Lobo. Controller, Processor & Data Protection Responsibilities. *WSI* : website. URL : https://www.wsiworld.com/blog/responsibilities-of-a-controller-processor-and-data-protection-officer-according-to-gdpr