Гайд “ЗНАЙОМСТВО З GDPR”

Вересень 2023

IAB Україна висловлює щиру подяку

Компанії MGID
генеральному медіа-партнеру
наших проєктів

Анастасія Байдаченко

CEO IAB Україна

GDPR довго залишався для української індустрії незнайомою абревіатурою, натомість незаперечний рух країни та її економіки в ЄС мотивує звернути пильну увагу до базових понять та вимог GDPR вже сьогодні. Адже адаптація індустрії не може бути миттєвою.

Проблематика GDPR, насамперед, питання юридичне, яке потребуватиме уваги юридичних відділів із відповідною кваліфікацією та досвідом спеціалістів. Проте це матиме безпосередній економічний вплив на результати діяльності компанії через систему істотних штрафів за порушення норм GDPR.

Проте ми у жодному разі не маємо обмежувати питання GDPR межами юридичних відділів, це первинна точка входу, проте розуміння та дотримання вимог це задача, яку мають вирішувати або бути обізнаними практично всі відділи організації.

Тож починаємо поступово готувати цифрову індустрію до нового рівня інтеграції з ЄС.

Хочу висловити щиру вдячність IAB Europe за надані напрацювання та гайди!

Загальний вступ до гайду

На сьогодні важко уявити сферу інтернет-бізнесу, на яку б не вплинули глобальні зміни регулювання обігу персональних даних в ЄС, що були привнесені GDPR. І сфера інтернет-реклами одна з найбільш чутливими до цих змін.

Визнаючи Україну природньою частиною європейського бізнес-середовища, а українських гравців світового ринку інтернет-реклами – його повноправними учасниками, IAB, у особі IAB Ukraine, переклав та адаптував Гайд до галузевого стандарту співробітництва учасників ринку інтернет-реклами до уваги всіх зацікавлених.

Цей документ містить опис основних понять, процесів та кроків, необхідних для послідовної, коректної та юридично захищеної взаємодії як з кінцевими користувачами на території ЄС, так і з бізнесами, зареєстрованими у державах-членах.

Ознайомившись із запропонованим Гайдом та запровадивши викладені в ньому практики на інструменти ви зможете не лише забезпечити формальну відповідність вашого бізнесу сучасним галузевим вимогам, але і побудувати стабільну і готову до розвитку інфраструктуру обробки персональних даних у своїй компанії.

Інструкція до гайду:

- До необхідного розділу Гайду можна перейти через посилання у Змісті
- До термінів, виділених синім кольором, даються роз'яснення безпосередньо в тексті документа чи на початку Гайду (Словник термінів, стор. 7)
- Зі статтями, на які є посилання в документі та Загальним регламентом захисту даних GDPR можна ознайомитися тут

Зміст

Огляд

27 квітня 2016 року Європейський Союз прийняв Загальний регламент про захист даних («**GDPR**» або «**Регламент**»), а вже 25 травня 2018 року GDPR став безпосередньо застосовною законодавчою нормою у Європейському Союзі (ЄС) та Європейській економічній зоні (ЄЕЗ), посиливши національні закони про захист даних.

GDPR поширюється не тільки на компанії, що базуються в ЄС, але і на компанії по всьому світу, які пропонують товари та послуги людям, що перебувають на території ЄС, або проводять моніторинг поведінки (профілювання) осіб на його території, або іншим чином здійснюють обробку персональних даних таких осіб.

GDPR регулює всі аспекти обробки персональних даних, які визначаються як будь-яку операцію або низку операцій з персональними даними або наборами персональних даних з використанням автоматизованих засобів або без них, такі як збирання, реєстрація, організація, структурування, зберігання, адаптація чи зміна, пошук, ознайомлення, використання, розкриття через передавання, розповсюдження чи надання іншим чином, упорядкування чи комбінування, обмеження, стирання чи знищення.

GDPR уповноважує відповідні органи стягувати значні адміністративні штрафи з підприємств, визнаних порушниками Регламенту. Залежно від тяжкості порушення, штрафи можуть сягати 20 000 000 євро або 4% від річного глобального обороту компанії — залежно від того, що більше.

Цей документ був підготовлений членами IAB Ukraine на основі матеріалів команди IAB Europe з виконання GDPR (**GIG**), щоб надати рекомендації українським компаніям щодо дотримання GDPR в правовій площині.

Словник термінів

Терміни, з якими вам слід спочатку ознайомитися; вони поширені у світі захисту персональних даних, але їх точне значення та контекст можуть дещо відрізнятися від того, якими спочатку вони здаються.

Персональні дані (Personal Data)	Такі закони, як GDPR або Закон України “Про захист персональних даних”, призначені для захисту лише персональних даних, і тому розуміння їх визначення є дуже важливим. GDPR надає дуже широке визначення персональних даних за задумом, і, як наслідок, GDPR має дуже широке застосування. Що робить щось персональними даними? Справа не в тому, які типи даних охоплюються, а в тому, що дані можуть розповісти вам про особу. Загалом, будь-які типи ідентифікаторів, які є унікальними для однієї особи, наприклад, ідентифікатори файлів cookie для відстеження, які використовуються для розпізнавання одного користувача на кількох веб-сайтах в Інтернеті, ймовірно, вважатимуться персональними даними. Персональні дані означають будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб’єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім’я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.
Обробка даних (Data Processing)	**Обробка даних (Data Processing)** Обробка даних (обробка персональних даних) - цей термін часто використовують у світі у законодавстві про захист персональних даних. Сам термін стосується майже будь-яких дій, які можна виконати з персональними даними. Фактично, визначення GDPR визначає обробку як «будь-яку операцію або набір операцій, які виконуються з персональними даними або наборами персональних даних, незалежно від того, автоматизовано чи ні». Це включає (але не обов’язково обмежується цим): «збір, фіксацію (запис), організацію, структурування, зберігання, адаптацію або зміну, пошук, консультування, використання, розкриття шляхом передачі, розповсюдження або іншим способом надання доступу, вирівнювання або комбінування, обмеження, видалення або знищення;» Навіть видалення персональних даних із вашої бази даних або серверів вважається обробкою персональних даних відповідно до GDPR, і тому важливо розуміти, які типи даних підпадають під визначення персональних даних, якщо ви «маєте» персональні дані як компанія та використовуєте їх під час ведення бізнесу, ви обробляєте їх та повинні дотримуватися принципів GDPR та Закону України “Про захист персональних даних”.
GDPR або Регламент	**Загальний регламент захисту даних 2016/679,** він же Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС. Це регламент в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Набув чинності 25 травня 2018 р.

Суб'єкт даних (Data subject)	Фізична особа, чиї персональні дані обробляються в ситуації, що підпадає під дію GDPR або Закону України “Про захист персональних даних”. Вона є «суб’єктом» персональних даних. У контексті онлайн-реклами ми зазвичай називаємо таких осіб «споживачами», «замовниками» та «користувачами Інтернету». **Контролер** - означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних. **Оператор** - визначається як фізична або юридична особа, державний орган, агентство або інший орган, який обробляє персональні дані від імені контролера.
Контролери та Оператори (Controllers and Processors)	Розмежування між Контролерами та Операторами в законодавстві про захист даних є надзвичайно важливим, оскільки воно покладає остаточну відповідальність за забезпечення захисту персональних даних. Контролери можуть приймати рішення щодо засобів, а також цілей обробки персональних даних. Як показують деякі рішення Суду ЄС, це поняття тлумачиться досить широко в GDPR, і для багатьох операцій з обробки персональних даних може існувати кілька спільних контролерів, які повинні розподіляти між собою різні обов’язки, що випливають з GDPR. Оператор — це особа, яку залучає контролер або група спільних контролерів для виконання конкретних завдань для контролера з персональними даними. Таким чином, вони не приймають рішення щодо засобів або цілей обробки персональних даних, а здійснюють це для контролера. Це може бути у випадку, коли оператор пропонує певну послугу від імені контролера, використовуючи персональні дані, надані контролером.
Перші особи	Видавці та інші постачальники онлайн-сервісів, які працюють з третіми особами для надання послуг на основі даних.
Треті особи	Партнери перших сторін.
Законна підстава (Legal Basis)	Згода та законні (легітимні) інтереси є двома типами «законної підстави» (legal basis). Законна підстава — це обґрунтування, необхідне відповідно до GDPR для обробки персональних даних. Без законної підстави обробка персональних даних жителів ЄС є незаконною; але це також стосується будь-якого бізнесу, який обробляє персональні дані в межах ЄС, незалежно від того, чи стосуються дані осіб у межах ЄС.
Робоча група (Робоча група із захисту даних)	Консультативна група, створена відповідно до ст. 29 Директиви, що трансформувалася в Європейську раду з захисту персональних даних (European data protection board) після набрання чинності GDPR у відповідності до ст. 68 GDPR.

Джерело: https://iabeurope.eu/privacy-data-protection/

Згода (Consent)	Згода є правовою підставою для обробки персональних даних, яка залежить від того, чи особи надають згоду особі або компанії, яка бажає обробляти їхні персональні дані. Концепція досить проста та зрозуміла, але GDPR визначає чотири умови, які мають бути виконані, перш ніж згода може вважатися дійсною: конкретна, поінформована, вільно надана та однозначна. У світі після GDPR багато організацій-видавців використовують платформи керування згодою («CMP»), щоб отримати згоду від імені видавця та залучених ним рекламних партнерів. Хочете дізнатися більше? Ознайомтеся з посібником щодо згоди IAB Europe.
Законний (легітимний) інтерес (Legitimate Interest)	Законний інтерес — це окрема правова підстава, яка не потребує попередньої згоди та має інші умови, а саме - те, що контролер може вказати свій законний інтерес; відповідна обробка персональних даних має бути необхідною для досягнення законного інтересу, а контролер повинен провести тест на баланс, щоб переконатися, що обробка персональних даних виправдана без згоди суб'єкта даних. Важливо мати на увазі, що хоча попередня згода суб'єкта даних (користувача) не є обов'язковою, йому все одно потрібно заздалегідь надати детальну інформацію про типи персональних даних, які збираються, мету цього збору та треті сторони, які отримають ці дані. Органи влади також проведуть аналіз кожного окремого випадку, щоб перевірити, чи є законний інтерес дійсним у разі проведення розслідувань або скарг.
Псевдонімізація	Означає обробку персональних даних у такий спосіб, що персональні дані більше не можна віднести до конкретного суб'єкта даних без використання додаткової інформації, за умови, що таку додаткову інформацію зберігають окремо, і на неї поширюється застосування технічних і організаційних інструментів для забезпечення того, що персональні дані не віднесено до фізичної особи, яку ідентифіковано чи можна ідентифікувати.
Ідентифікатор користувача або UID	Це псевдонімний ідентифікатор користувача, такий як ідентифікатор cookie або мобільний ідентифікатор реклами (наприклад, IDFA в iOS). UID, який використовується для постійної ідентифікації браузера, комп'ютера або пристрою, відповідно до GDPR вважається "цифровим ідентифікатором" і є персональними даними.
Профілювання	Будь-яка форма автоматизованої обробки персональних даних із оцінюванням персональних аспектів, що стосуються фізичної особи, зокрема для аналізу або передбачення аспектів, що стосуються продуктивності суб'єкта даних на роботі, економічної ситуації, здоров'я, особистих уподобань або інтересів, надійності або поведінки, місцезнаходження або пересування.
PBD	Конфіденційність (приватність) за проєктуванням (privacy by design).

Джерело: https://iabeurope.eu/privacy-data-protection/

Директива	**Директива 95/46/ЄС** Європейського Парламенту і Ради Європейського Союзу від 24 жовтня 1995 р. про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних.
e-Commerce Директива	**Директива про електронну торгівлю 2000/31/ЄС** Європейського Парламенту і Ради Європейського Союзу від 08 червня 2000 р., яка регулює структуру внутрішнього ринку для онлайн-послуг, певні правові аспекти послуг інформаційного суспільства, зокрема електронної комерції.
e-Privacy Директива	**Директива 2002/58/ЄС** Європейського Парламенту і Ради Європейського Союзу від 12 липня 2002 року щодо обробки персональних даних і захисту приватності в секторі електронних комунікацій.
e-Privacy Регламент	**Регламент щодо приватності та електронних комунікацій,** пропозиція щодо регулювання питань, пов'язаних із приватністю, переважно щодо електронних комунікацій у межах Європейського Союзу, який має на меті замінити собою ePrivacy Директиву та надавати уточнення до GDPR.
TCF або **Протокол**	Протокол прозорості та згоди IAB Europe
EDPB	European Data Protection Board/ Європейська рада із захисту персональних даних.
GIG IAB Europe	Група IAB Europe з виконання GDPR
DPO	Відповідальна особа з питань захисту персональних даних.
RTB	Торги у режимі реального часу.
DPIA (Data Protection Impact Assessment)	Оцінка впливу на захист персональних даних
LIA	Оцінка законних інтересів
TCF/ППЗ	Протокол Прозорості та Згоди IAB Europe (Transparency & Consent Framework).
CMP/ПАЗ	Платформа адміністрування згоди (Consent Management Platform)
GVL	Глобальний список постачальників (Global Vendor List)

Джерело: https://iabeurope.eu/privacy-data-protection/

Шлях до дотримання GDPR

Робочий документ №1

Зміст

- Шлях до дотримання GDPR
- Що потрібно документувати
- Створення та виконання Плану дотримання GDPR
- Розгляд Протоколу прозорості та згоди IAB Europe
- Проведення аналізу впливу на захищеність даних
- Перегляд та зміна наявних договорів з постачальниками та політик приватності (конфіденційності)
- Призначення Відповідальної особи з питань захисту персональних даних (DPO)
- Використання «єдиного вікна»
- Підтримання поінформованості та контроль дотримання GDPR

*Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf

Шлях до дотримання GDPR

Облік та документування діяльності з обробки даних та заходів безпеки

Підзвітність та облік є центральною темою GDPR. Облік та документування всіх ваших дій з обробки даних та застосовуваних заходів безпеки є належним першим кроком до цієї мети.

У рамках цього процесу також потрібно визначити, **мету** і **спосіб** обробки наявних у вас персональних даних. Щоб мати базове розуміння щодо діяльності з обробки персональних даних, потрібна увага до певних аспектів, особливо якщо ви опрацьовуєте чутливі персональні дані.

Крім того, при започаткуванні обліку може виявитись, що саме ваш тип обробки даних вимагає спеціальних заходів захисту, тому, залежно від характеру обробки даних, застосовні вами заходи безпеки, також можуть потребувати ретельної оцінки та дослідження.

Це необхідний крок, враховуючи розмір штрафів, які можуть бути накладені на компанії у разі порушення, та інші санкції, яким можна було б запобігти або які можна було б пом'якшити за умови використання більш відповідних безпекових процедур та механізмів.

Належний підхід в цьому випадку — залучити до задачі різні відділи вашої компанії**. Бажано уникати ситуації, коли дотримання GDPR залишається виключно справою юридичних відділів компанії, відповідальної особи з питань захисту персональних даних (DPO) або IT відділу, адже питання приватності пов'язане чи не з кожним відділом компанії.**

Проведення інтерв'ю та анкетування працівників усіх відділів— і, можливо, ключових контрагентів та партнерів — дозволяють визначити, який тип обробки даних проводиться в кожній сфері роботи вашої компанії.

Розуміння всіх цих процесів є основоположним. Це дозволяє вам як компанії фіксувати кожен тип обробки персональних даних відповідно до мети, що забезпечує важливість схем обробки даних і подальше дотримання GDPR.

**Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf*

Що потрібно документувати

Започатковуючи облік та документування процедур з обробки даних, потрібно розглянути всі процеси в компанії та відповісти на питання «що», «де», «коли», «чому», а також передбачити очікувані наслідки для кожного процесу та провести аналіз ризиків.

Варто враховувати, що це також стосується будь-яких даних працівників, які ви обробляєте. Наступні питання можуть допомогти вам у цьому процесі:

- Яка інформація надається перед збором та обробкою даних?
- Які дані ви обробляєте та щодо якого кола осіб, де саме і коли здійснюється обробка, яка мета такої обробки? (Чи є у вас правові підстави для цього; і чи здійснюється обробка відповідно до основних принципів **обробки даних**)?
- Які дані підлягають анонімізації, а які – псевдонімізації?
- Як довго ви зберігаєте такі дані?
- З ким ви ділитеся такими даними?
- Які ризики несе кожен з цих процесів?
- У яких випадках ваш бізнес є Контролером, Оператором або спільним контролером даних?
- Чи обробляє ваша компанія те, що **будь-яка** держава ЄС вважатиме персональними даними (наприклад, IP-адреса, файл cookie, будь-який онлайн-ідентифікатор)?
- Чи процес відбувається з урахуванням міркувань безпеки? Якщо так, задокументуйте конкретні відомості про це.
- Зверніть увагу, що будь-які персональні дані, які зберігаються або передаються за межі ЄС, повинні відповідати Правилам транскордонної передачі даних (розділ 13 GDPR).
- Чи отримує ваша компанія згоду та надсилаєте її своїм операторам та іншим третім особам? Чи отримана згода потрібна тільки вашій компанії, чи вашим третім особам також?
- Перевірте та задокументуйте процедури безпеки.
- Ваша компанія, як і будь-яка компанія, що виступає в якості вашого оператора, суб-оператора або **спільного** контролера даних, забезпечує безпеку даних? Згідно з GDPR, про порушення безпеки даних потрібно повідомити контролюючий орган із приватності даних протягом 72 годин після виявлення інциденту. Якщо у вас ще немає плану реагування на безпекові інциденти, його потрібно створити. Розгляньте можливість створення шаблонів-повідомлень на такий випадок.

**Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf*

Створення та виконання Плану дотримання GDPR

Запропонований «аудит даних» має на меті допомогти вам виявити діяльність, яка — частково або в цілому — може суперечити GDPR і, отже, вимагає змін.

Під час цього процесу слід розглянути наступні питання:

- Яким чином ваші поточні процеси можуть суперечити GDPR і які зміни в процеси обробки потрібно внести, щоб вирішити цю проблему?
- Скільки часу знадобиться на внесення необхідних змін?
- Чи обробляєте ви дані на основі згоди користувачів? Чи використовуєте ви стандартизований метод отримання та передачі згоди третім особам та операторам?
- Чи потрібно створювати додаткові логи? Наприклад, якщо дані обробляються на основі згоди користувачів, зазначати час, коли згода була надана, не надана або відкликана (пов'язана з IP-адресою, файлом cookie та/або іншим ідентифікатором).
- Як ви будете поводитись з «правами доступу» користувача та іншими правами суб'єкта даних (глава III GDPR, статті 12-22) та підтримувати відповідність?
- Працюйте зі своїми операторами та суб-операторами чи спільними контролерами, щоб створити задокументовані інструкції щодо обробки даних (необхідно укласти відповідні угоди щодо обробки персональних даних з відповідними операторами, суб-операторами чи спільними контролерами даних).

**Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf*

Розгляд Протоколу прозорості та згоди IAB Europe

Протокол прозорості та згоди IAB Europe («**TCF**» або «**Протокол**») має просту мету — допомогти всім сторонам у ланцюжку цифрової реклами забезпечити дотримання Регламенту та Директиви ЄС “Про приватність та електронні комунікації” при обробці персональних даних або доступі та/або зберіганні інформації на пристрої користувача, такої як файли cookie, рекламні ідентифікатори, ідентифікатори пристроїв та інші технології відстеження.

Особливо актуальним Протокол є для «перших осіб», таких як видавці та інші постачальники онлайн-сервісів, які працюють з третіми особами для надання послуг на основі даних.

Використовуючи TCF, перші особи уможливлюють обробку даних користувачів третіми особами на одній з законних правових підстав Регламенту.

Протокол стандартизує подання запитів користувачів на обробку даних третьою особою, які вимагають «інформованої» згоди на обробку даних. Протокол дозволяє «сигналізувати» про вибір користувача всьому ланцюжку постачання реклами.

TCF - це некомерційне адміністрування галузі з використанням відкритого коду, що засноване на консенсусі всіх учасників ринку на чолі з IAB Europe при значній підтримці з боку IAB Tech Lab, яке забезпечує технічне управління відкритим вихідним кодом специфікацій і контролем версій.

Компаніям варто вирішити чи хочуть вони використовувати Протокол для власних потреб щодо дотримання законодавства. Використання Протоколу особливо допоможе тим компаніям, які розраховують на згоду у якості правової підстави для здійснення обробки даних.

Коментар юриста:
Варто звернути увагу на оновлену версію TCF 2.2 (запущений в травні 2023 року), який враховуючи наслідки прецедентного права, а також інструкцій органів із захисту даних (DPA) виставляє до учасників ринку ще більші вимоги щодо захисту даних.

*Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf

Проведення аналізу впливу на захищеність даних

GDPR вимагає від контролерів даних проводити оцінку впливу на захист персональних даних (англійською в оригіналі тексту GDPR «Data Protection Impact Assessment» та скорочено надалі - «**DPIA**») перед початком будь-якої нової діяльності з обробки даних у таких випадках:

- Якщо впроваджується нова технологія;
- Якщо обробка, ймовірно, матиме високий ризик для суб'єктів даних. Ви можете використовувати один аналіз для декількох операцій з обробки, якщо вони супроводжуються схожими ризиками;
- Якщо обробка передбачає систематичну та широку оцінку особистісних деталей щодо фізичних осіб, яка базується на автоматизованій обробці, включаючи профілювання, і обґрунтовує рішення з правовими наслідками щодо фізичної особи або аналогічним чином суттєво впливає на фізичну особу;
- Якщо ваша компанія обробляє велику кількість чутливих персональних даних;
- Якщо ваша компанія систематично моніторить публічний простір у великих масштабах.

Зверніть увагу на роботу уповноважених органів — їм доручено скласти загальнодоступний перелік заходів з обробки, які потребують аналізу. Вони ж можуть опублікувати і «білий список» операцій з обробки, які не вимагають аналізу.

*Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf

Перегляд та зміна наявних договорів з постачальниками та політик приватності (конфіденційності)

Перегляд та зміна ваших внутрішніх процесів, де це необхідно, є лише частиною процесу налаштування відповідності GDPR. Ще одним важливим елементом є забезпечення відображення цих процесів в договорах з партнерами.

У деяких випадках GDPR вимагає, щоб ви мали спеціальні угоди з компаніями, з якими ви працюєте, наприклад, коли ваша компанія та інша компанія вважаються «спільними контролерами». Нагадаємо, що контролером даних є той, хто визначає **мету** і **засоби** обробки персональних даних.

Варто переглянути вже наявні контракти з постачальниками та власну політику **приватності (конфіденційності).** Рекомендуємо:

- Переглянути всі контракти з постачальниками та внести зміни, якщо це необхідно.
    - При роботі з декількома операторами даних повинна бути створена «домовленість» між суб-операторами чи групою операторів для розподілу обов'язків щодо дотримання захисту даних між собою.

- Переглянути свої угоди з кінцевими користувачами (правила користування).
- Переглянути свої повідомлення про приватність даних (зовнішнє розкриття) та політики щодо приватності (конфіденційності) (внутрішні правила).
    - Вам варто мати правила та процедури для працівників, які працюють з персональними даними, і документувати їх у політиках щодо приватності (конфіденційності).
    - Суб'єктам даних повинна бути надана певна інформація про збір та подальшу обробку їх персональних даних. Ця інформація повинна бути надана в «стислій, прозорій, зрозумілій та легкодоступній формі, з використанням чіткої та зрозумілої мови […]» – зазвичай у формі повідомлення про приватність (конфіденційність) даних.
    - Для суб'єктів даних повинен бути доступний короткий зміст домовленості спільних контролерів.

Ви можете розглянути можливість використання інструментів або програмного забезпечення для моніторингу виконання узгодженого договору та політики щодо приватності (конфіденційності) залученими третіми особами. Існує широкий спектр ринкових рішень контролю витоку даних, управління тегами, інструментів підтримання приватності, засобів запобігання втраті даних тощо.

*Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf

Призначення відповідальної особи з питань захисту персональних даних (DPO)

GPDR вимагає від компаній призначати відповідальну особу з питань захисту персональних даних (англійською в оригіналі тексту ”data protection officer», скорочено та надалі «DPO»):

- Якщо цього вимагає законодавство держави ЄС, де компанії зареєстровані;
- Якщо основною діяльністю компанії є обробка, що стосується регулярного та систематичного моніторингу суб'єктів даних у великих масштабах;
- Якщо обробка персональних даних є основною діяльністю і передбачає регулярний та систематичний моніторинг суб'єктів даних у великих масштабах; або оброблювані дані належать до чутливої інформації, що розкриває расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, членство в професійних спілках, дані стосовно стану здоров’я або статевого життя фізичної особи чи її сексуальної орієнтації, обробляє генетичні або біометричні дані виключно з метою ідентифікації фізичної особи.

На DPO покладено завдання по забезпеченню поінформованості компанії про свої зобов’язання щодо захисту персональних даних та нагляд за дотриманням компанією таких зобов’язань. DPO повинні володіти експертними знаннями законодавства та практик захисту персональних даних і мати можливість виконувати наступні функції:

- Інформувати та консультувати контролера або оператора (і будь-яких співробітників, які залучені до обробки персональних даних) про їх зобов'язання відповідно до GDPR;
- Слідкувати за дотриманням GDPR контролером або оператором;
- Консультувати щодо проведення Аналізу та брати участь у попередніх консультаціях з уповноваженими органами із захисту персональних даних;
- Співпрацювати з уповноваженими органами із захисту персональних даних та діяти як контактна особа;
- Своєчасно вирішувати всі питання захисту персональних даних, що стосуються контролера або оператора. Контролер або оператор повинні надати DPO необхідні ресурси та підтримку для цього.

DPO може бути штатним співробітником компанії або зовнішнім консультантом; GDPR передбачає, що групи компаній можуть призначити одну DPO, якщо DPO може повноцінно виконувати свої функції для кожної з цих компаній. DPO зобов'язана дотримуватися конфіденційності щодо своєї роботи, а також має захищений статус щодо свого роботодавця. Організація не може інструктувати DPO щодо виконання її обов'язків, не може звільнити DPO, або застосовувати будь-які інші дисциплінарні заходи внаслідок несумлінного виконання нею своїх обов'язків.

*Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf

Використання «єдиного вікна»

Однією з потенційних переваг, які GDPR може надати компаніям, є концепція «єдиного вікна». Це стосується організацій з декількома установами у різних країнах ЄС, або взагалі не зареєстрованих в жодній із країн ЄС, оскільки це дозволяє їм призначати «керівний наглядовий орган». В таких випадках компанії повинні ретельно зважити свої варіанти щодо вибору «єдиного вікна».

Відповідно до GDPR, орган з приватності персональних даних країни ЄС, де організація має свою «основну установу», буде її «керівним органом».

Керівний орган має повноваження регулювати цю організацію в усіх державах-членах. Щоб претендувати на «єдине вікно», організація потребує «місця для основної установи» в межах ЄС. “Основною установою”, як правило, є європейська штаб-квартира компанії, але відповідно до законодавства ЄС про компанії це може змінюватися залежно від ситуації.

Наявність «єдиного вікна» та керівного органу з приватності персональних даних як єдиного контактного пункту (на противагу роботі з уповноваженими органами з приватності даних в декількох державах-членах одразу й одночасно) дозволить більш уніфіковано забезпечувати відповідність законодавству на ринках ЄС.

У випадку відсутності представництв в ЄС також є можливість залучити законного представника на території ЄС на контрактній основі й таким чином скористатися всіма перевагами «єдиного вікна».

*Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf

Підтримання поінформованості та контроль дотримання

Ви повинні навчати та інформувати своїх співробітників про наслідки порушення GDPR та вашої нової політики дотримання **приватності (конфіденційності)** для їхньої роботи та переконатися, що дотримання ваших внутрішніх політик забезпечується за допомогою відповідних дисциплінарних заходів, де це необхідно.

Залишайтеся в курсі галузевих ініціатив та стандартів, приєднуйтесь та взаємодійте з IAB Europe та IAB на ринках, де ви працюєте, а також стежте за роботою Європейської наглядової ради з приватності персональних даних та уповноважених органів з приватності даних на ринках, де ви працюєте.

Також важливо своєчасно інформувати своїх партнерів про будь-які зміни, які ви вносите у свої продукти або послуги в результаті ваших заходів щодо дотримання GDPR.

Якщо ваша організація працює з клієнтами, вони також повинні бути проінформовані про оновлення політики щодо **приватності (конфіденційності).**

Зокрема, коли йдеться про використання згоди як правової підстави для обробки персональних даних, надзвичайно важливо повідомляти всім залученим сторонам про нові процеси.

- Інформуйте співробітників, операторів, користувачів, клієнтів про зміни у ваших угодах з кінцевими користувачами та політиці щодо конфіденційності.

- Інформуйте постачальників, операторів, суб-операторів, спільних контролерів про необхідні зміни договорів з ними.

.

*Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180906_IABEU-GIG-Working-Paper01_Compliance-Primer_v1.1.pdf

Визначення персональних даних відповідно до GDPR

Робочий документ №2

Зміст

- Основні положення
- Персональні дані за GDPR
- Персональні дані
- Анонімні дані
- Псевдонімізовані дані
- Спеціальні категорії персональних даних
- Висновок

https://iabeurope.eu/wp-content/uploads/2019/08/20170719-IABEU-GIG-Working-Paper02_Personal-Data.pdf

Основні положення

- Визначення персональних даних відповідно до GDPR є дуже широким і навмисно всеохопним. Псевдонімізовані дані визначаються як підкатегорія персональних даних і все ще вимагають повного застосування GDPR.

- Файли cookie та інші засоби та онлайн-ідентифікатори (IP-адреси, IDFA, AAID тощо) прямо називаються прикладами персональних даних відповідно до GDPR. Завдяки цьому широкому визначенню дуже ймовірно, що будь-які дані, що обробляються в екосистемі онлайн-реклами, підпадають під визначення персональних даних. Оскільки визначення є надзвичайно широким, краще перестрахуватися та припустити, що дані є персональними.

- Якщо може здатися, що дані не входять в рамки персональних даних, слід провести ретельний аналіз, щоб обґрунтувати це в кожному конкретному випадку. Залежно від обставин, одна й та ж частина даних (тобто IP-адреса) може бути особистими, псевдонімізованими або анонімними даними. Це залежить від обставин, в яких IP-адреса отримується, для яких цілей вона використовується, і хто отримує IP-адресу

https://iabeurope.eu/wp-content/uploads/2019/08/20170719-IABEU-GIG-Working-Paper02_Personal-Data.pdf

Персональні дані відповідно до GDPR

Визначення «персональних даних» є фундаментальним для законів про захист даних, оскільки GDPR стосується лише персональних даних. Дані, які не є персональними даними, виходять за рамки застосування GDPR.

Хоча сфера цифрової реклами та інші бізнеси, які використовують подібні технології, часто інтерпретують унікальні онлайн-ідентифікатори, наприклад, ідентифікатори cookie та рекламні ідентифікатори мобільних пристроїв, як такі, що виходять за рамки застосування закону про захист персональних даних, коли вони не поєднуються з особистими ідентифікаційними даними (такими як ім'я або адреса електронної пошти), ці онлайн-ідентифікатори, ймовірно, підпадають під сферу персональних даних відповідно до GDPR в залежності від обставин.

Тому вкрай важливо, щоб компанії, які займаються цифровою рекламою, розуміли, як до них застосовується визначення персональних даних в GDPR.

У цій статті розглядається сфера застосування персональних даних відповідно до GDPR, включаючи поняття анонімних даних (які не є персональними даними та не регулюються GDPR) та **псевдонімізованих даних** (які є персональними даними та регулюються GDPR).

https://iabeurope.eu/wp-content/uploads/2019/08/20170719-IABEU-GIG-Working-Paper02_Personal-Data.pdf

Персональні дані

Визначення персональних даних в GDPR розширює текст визначення, що міститься в Директиві про захист даних (Директива 95/46/ЄС, надалі «**Директива**»), явно посилаючись на додаткові приклади ідентифікаторів, таких як онлайн-ідентифікатори та фактори, які можуть бути використані для ідентифікації особи. Стаття 4(1) GDPR говорить наступне:

«Персональні дані - означає будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами ***як ім'я, ідентифікаційний номер, дані про місце перебування, онлайн-ідентифікатор*** *або за одним чи кількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи».*

Преамбули GDPR (26) і (30) надають додаткову інформацію щодо визначення персональних даних. Преамбула GDPR (26) представляє концепцію, згідно з якою особу можна ідентифікувати, «виокремлюючи» цю особу, прямо чи опосередковано. Це вказує на те, що необхідно враховувати всі засоби, які обґрунтовано ймовірно будуть використані для ідентифікації особи, враховуючи всі об'єктивні фактори при такому визначенні. У преамбулі 26 зазначається:

«...Щоб встановити можливість ідентифікації фізичної особи, необхідно взяти до уваги всі способи, що будуть використані з високою ймовірністю, такі як виділення контролером або іншою особою для ідентифікації фізичної особи прямо чи опосередковано. Для встановлення достатньої ймовірності використання способів для ідентифікації фізичної особи, необхідно взяти до уваги всі об'єктивні фактори, такі як витрати та період часу, необхідні для ідентифікації, з огляду на технології, наявні станом на момент обробки, і технологічні розробки».

У преамбулі GDPR (30) вказано, що ідентифікація може відбуватися шляхом пов'язання онлайн-ідентифікаторів, таких як ідентифікатори файлів cookie та IP-адреси, з іншою інформацією для створення профілів. У преамбулі GDPR (30) зазначається:

«Фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, додатків, інструментів чи протоколів, ***зокрема IP-адрес, ідентифікаторів cookie або інших ідентифікаторів, таких як мітки радіочастотної ідентифікації.*** *Це може залишити підказки, які, особливо в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою з серверів,* ***можна використати для створення профілів фізичних осіб та їхньої ідентифікації****»*

Персональні дані

Ці положення значно розширюють поняття персональних даних від загальноприйнятих тлумачень відповідно до Директиви. Хоча сфера цифрової реклами часто інтерпретує унікальні онлайн-ідентифікатори, такі як ідентифікатори cookie, як такі, що виходять за рамки законодавства про захист персональних даних, коли вони не поєднуються з особистими ідентифікаційними даними (такими як ім'я або адреса електронної пошти), ці онлайн-ідентифікатори, ймовірно, підпадають під сферу застосування персональних даних відповідно до GDPR за багатьох обставин.

Як описано в преамбулі GDPR (26), потрібно буде розглянути всі способи, які будуть використані з високою ймовірністю, щоб ідентифікувати основну фізичну особу, щоб визначити, чи є дані персональними даними; однак, як правило, відповідно до GDPR, такі дані, як онлайн-ідентифікатори, повинні розглядатися як персональні дані, якщо не може бути наведено обґрунтований аргумент про те, що суб'єкт даних не може бути (прямо або опосередковано) ідентифікованим і не може бути виокремленим.

Визначення того, чи є частина даних персональними даними, залежить від контексту. Наприклад, IP-адреса, яка відповідає загальнодоступній точці, такій як кав'ярня, і використовується сотнями клієнтів щодня, сама по собі навряд чи містить персональні дані. Однак, якщо компанія пов'язує цю загальну IP-адресу з іншою інформацією, яка дозволила б ідентифікувати одну особу, то IP-адреса, ймовірно, буде вважатися персональними даними.

Аналогічно, скорочена IP-адреса не буде персональними даними, якщо власник цієї скороченої IP-адреси не має раціональних засобів для ідентифікації особи. Однак, якщо власник скороченої IP-адреси може, використовуючи раціональні засоби, що перебувають у його розпорядженні, зібрати додаткову інформацію, яка дозволила б ідентифікувати особу, то навіть ця скорочена IP-адреса, ймовірно, буде персональними даними.

Компанії повинні пам'ятати, що персональні дані охоплюють більше даних, ніж те, що зазвичай вважається особистою інформацією в деяких юрисдикціях за межами ЄС. У випадках, коли незрозуміло, чи є дані персональними даними, буде доцільніше ставитись до них як до персональних даних, особливо з огляду на потенціал високих штрафів відповідно до GDPR.

Анонімні дані

Як і в Директиві до цього, GDPR не поширюється на анонімні дані. У преамбулі GDPR (26) пояснюється, що анонімна інформація не стосується особи, яку ідентифіковано або можна ідентифікувати. У преамбулі GDPR (26) зазначається:

«Принципи захисту даних, відповідно, не можна застосовувати до анонімної інформації, зокрема інформації, що не стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати, або персональних даних, що стали анонімними у такий спосіб, що суб'єкта даних неможливо чи більше неможливо ідентифікувати. Таким чином цей Регламент не стосується обробки такої анонімної інформації, у тому числі, для статистичних або дослідницьких цілей».

Робоча група Статті 29 GDPR у своєму попередньому Висновку 05/2014 про методи анонімізації зазначила, що анонімізація — це «метод, що застосовується до персональних даних з метою досягнення **незворотної де-ідентифікації**». У цьому висновку викладено різні методи анонімізації та підкреслено, що «тематичні дослідження та дослідницькі публікації показали, наскільки важко створити справді анонімний набір даних і зберегти при цьому стільки основної інформації, скільки потрібно для виконання завдання».

Якщо компанія зберігає дані, які є дійсно анонімними, GDPR не застосовується до цих даних. Наприклад, частина загальної інформації про місцезнаходження, яка не ідентифікує особу, є анонімними даними, які не підпадають під дію GDPR. Якщо компанія володіє назвою великого міста (наприклад, Брюссель), не пов'язує будь-яку іншу ідентифікаційну інформацію і не може отримати або використовувати додаткову інформацію, яка могла б пов'язати місцезнаходження з особою, то дані є анонімними.

Агреговані дані, які не стосуються одного користувача, але стосуються цілої групи користувачів, є анонімними даними до тих пір, поки особи, чиї дані знаходяться в пулі, не можуть бути ідентифіковані.

Аналіз того, чи є певна частина інформації або група інформації анонімною, залежить від контексту і не завжди функціонує зрозуміло. Якщо компанія не впевнена, чи є дані, які вона зберігає, персональними даними або анонімними даними, обробка даних як персональних даних буде найбільш раціональним рішенням.

https://iabeurope.eu/wp-content/uploads/2019/08/20170719-IABEU-GIG-Working-Paper02_Personal-Data.pdf

Псевдонімізовані дані

GDPR вводить концепцію псевдонімізованих даних як підмножини персональних даних, які не можна віднести до конкретного суб'єкта даних без додаткової інформації. У статті 4(5) зазначено:

Псевдонімізація *- означає* обробку *персональних даних у такий спосіб, що персональні дані більше не можна віднести до конкретного суб'єкта даних без використання додаткової інформації, за умови, що таку додаткову інформацію зберігають окремо, і на неї поширюється застосування технічних і організаційних інструментів для забезпечення того, що персональні дані не віднесено до фізичної особи, яку ідентифіковано чи можна ідентифікувати».*

Псевдонімізація не розглядалася в Директиві, і багато хто в рекламній сфері вважає, що псевдонімізовані дані виходять за рамки персональних даних в Директиві й, отже, за межі сфери дії Директиви. Відповідно до GDPR, використання псевдонімів не робить набір даних анонімним (не виводить їх за межі дії GDPR). У преамбулі GDPR (26) уточнюється, що псевдонімізовані дані входять до сфери дії GDPR:

«...Персональні дані, які пройшли псевдонімізацію, що можна присвоїти фізичній особі після використання додаткової інформації, необхідно розглядати як інформацію про фізичну особу, яку можна ідентифікувати...»

Однак, як описано в статті 11 GDPR, використання псевдонімних даних може виключати дані з певних зобов'язань GDPR, які конкретно вимагають ідентифікації, таких як доступ суб'єкта та право на виправлення, видалення та **перенесення** даних (статті 15-20). **Онлайн-ідентифікатори, такі як ідентифікатори cookie, пов'язані з історією веб-перегляду в Інтернеті, часто є персональними даними відповідно до GDPR, хоча завжди необхідно аналізувати конкретну ситуацію.**

Псевдонімізація визнається запобіжником, який зменшує ризики для суб'єктів даних і допомагає контролерам і операторам виконувати свої зобов'язання щодо захисту даних. У преамбулі GDPR (28) визнається ця перевага використання псевдонімів і зазначається, що:

«Псевдонімзація персональних даних може зменшити ризики для відповідних суб'єктів даних та допомогти контролерам і операторам у виконанні своїх обов'язків із захисту персональних даних. Пряма псевдонімізація у цьому Регламенті не передбачає обмеження будь-яких інших заходів щодо захисту даних».

https://iabeurope.eu/wp-content/uploads/2019/08/20170719-IABEU-GIG-Working-Paper02_Personal-Data.pdf

Псевдонімізовані дані

GDPR чітко визнає псевдонімізацію як запобіжний захід, який може сприяти допустимій обробці для вторинного використання. У статті 6(4) GDPR зазначається:
«Якщо обробка для іншої цілі, ніж тієї для якої відбувалося збирання персональних даних, не заснована на згоді суб'єкта даних або на законодавстві Союзу чи держави-члена, що є необхідним і пропорційним заходом у демократичному суспільстві для гарантування цілей, вказаних у статті 23(1), контролер, для того, щоб переконатися, чи є обробка для іншої цілі сумісною із ціллю первинного збирання персональних даних, повинен врахувати, між іншим: ... (e) ***наявність належних гарантій, що можуть передбачати шифрування чи псевдонімізацію****».*

Стаття 89(1) GDPR визнає псевдонімізацію гарантією обробки для архівування в суспільних інтересах, наукових або історичних дослідницьких цілях або статистичних цілях. У статті 89(1) GDPR зазначено:
*«*Обробка *для досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження або статистичних цілей підлягає застосуванню відповідних гарантій, згідно з цим Регламентом, для прав і свобод суб'єкта даних. Такі гарантії забезпечують наявність технічних і організаційних інструментів, зокрема, для забезпечення дотримання принципу мінімізації даних. Такі заходи можуть передбачати* псевдонімізацію *за умови можливості досягнути у такий спосіб зазначених цілей. Якщо таких цілей можна досягнути у процесі подальшої обробки даних, що не дозволяє чи більше не дозволяє ідентифікацію суб'єктів даних, зазначені цілі досягають у вказаний спосіб».*

Важливо, що GDPR визнає, що псевдонімізація персональних даних можлива з боку контролера, якщо цей контролер зберігає додаткову інформацію, яка може бути використана для присвоєння цих даних окремому суб'єкту даних, до тих пір, поки контролер вживає технічних та організаційних заходів для збереження цієї інформації окремо. У преамбулі 29 GDPR зазначається:

«Для створення стимулів псевдонімізації під час обробки персональних даних, заходи щодо псевдонімізації повинні, дозволяючи при цьому загальний аналіз, уможливлювати їхнє використання самим контролером, якщо такий контролер застосував технічно-організаційні інструменти, необхідні для забезпечення, у відповідній ситуації обробки, виконання цього Регламенту, а також ***якщо додаткову інформацію для приписування персональних даних до певного суб'єкта даних зберігають окремо****. Контролер, що здійснює обробку персональних даних, повинен зазначити уповноважених осіб серед тих, що працюють з тим самим контролером»*

Псевдонімізовані дані

Стаття 25(1) GDPR визнає, що технічні та організаційні заходи, такі як псевдонімізація, повинні розроблятися «у момент визначення засобів обробки та в момент власне обробки». Ця конструкція підтримує дві однаково важливі концепції псевдонімізації.

По-перше, це збір даних таким чином, щоб контролер міг зберігати дані, які не можуть бути віднесені до конкретного суб'єкта даних без використання додаткової інформації. Іншими словами, дані є псевонімізованими при їх зборі, використанні та зберіганні. Наприклад, деякі компанії в сфері цифрової реклами ніколи не збирають інформацію, щоб безпосередньо ідентифікувати кінцевого користувача; швидше, вони збирають лише випадковий ідентифікатор cookie та відвідані пов'язані URL-адреси, що дозволяють розпізнати браузер, але кінцевий користувач не може бути безпосередньо ідентифікований. Ці дані є псевдонімізованими для цієї компанії в сфері цифрової реклами, оскільки ця компанія не має реального прямого доступу до додаткової інформації, яка дозволила б їй безпосередньо ідентифікувати суб'єкта даних.

Друга концепція псевдонімізації — це процес, який компанії можуть застосовувати до персональних даних, наприклад, з використанням методів шифрування, хешування або токенізації, щоб гарантувати, що дані не пов'язані з фізичною особою, яку можна ідентифікувати. Наприклад, компанія може збирати повне ім'я, поштову адресу, номер рахунку та відвідані URL-адреси. Якщо вона зберігає цю інформацію в своїй базі даних абонентів, вона може створити окрему базу даних, яка була псевдонімізована шляхом видалення інформації про ім’я, поштову адресу та хешування номера рахунку. Якщо компанія вживає відповідних технічних та організаційних заходів для збереження баз даних окремо та запобігання повторному віднесенню псевдонімізованих даних, то друга база даних є псевдонімізованою базою даних, яка може, наприклад, використовуватися для дослідницьких цілей у безпечний для конфіденційності спосіб.

.

Псевдонімізовані дані

IP-адреса є прикладом даних, які можуть бути анонімними даними, псевдонімізованими персональними даними або неанонімними персональними даними, залежно від конкретних обставин. Згаданий раніше в цій статті приклад загальної IP-адреси в точці спільного використання є анонімними даними, коли вони зберігаються без будь-якої іншої інформації, оскільки вона не ідентифікує особу або не робить можливою ідентифікацію особи. Крім того, згаданий раніше в цій статті приклад скороченої IP-адреси, яка сама по собі не є персональними даними, але стає персональними даними, якщо власник цієї скороченої IP-адреси може обґрунтовано пов'язати скорочену IP-адресу з додатковою інформацією, щоб дозволити власнику ідентифікувати особу. Якщо єдиними додатковими даними, які зберігаються, є відсутній октет, то дані будуть псевдонімізованими персональними даними; однак, якщо додатковими даними, які зберігаються, є відсутній октет плюс інформація, така як ім'я та адреса, пов'язані з IP-адресою, то ці об'єднані дані будуть неанонімними персональними даними. **Компаніям рекомендується ретельно аналізувати групи даних, які вони зберігають, щоб визначити, чи є вони персональними даними в конкретному випадку.**

.

Спеціальні категорії персональних даних

GDPR, як і Директива, визнає певні спеціальні категорії персональних даних, які не можуть бути опрацьовані, якщо не виконуються суворі вимоги (що містяться в статті 9(2)), такі як явна згода суб'єкта даних.

Стаття 9(1) GDPR визначає спеціальні категорії чутливих даних як: «персональні дані, що розкривають расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, чи членство в професійних спілках, і обробка генетичних даних, біометричних даних для цілі єдиної ідентифікації фізичної особи, даних стосовно стану здоров'я чи даних про статеве життя фізичної особи чи її сексуальної орієнтації».

Дані, що стосуються кримінальних вироків і правопорушень, також підлягають обмеженням. Стаття 10 GDPR, як і Директива, обмежує її опрацювання контролем офіційних органів або випадками, коли національне законодавство може передбачати пом'якшення вимог.

Компанії, які бажають обробляти спеціальні категорії персональних даних або даних, що стосуються кримінальних правопорушень, повинні обов'язково дотримуватися більш жорстких вимог до обробки таких даних.

https://iabeurope.eu/wp-content/uploads/2019/08/20170719-IABEU-GIG-Working-Paper02_Personal-Data.pdf

Висновок

GDPR розширює визначення персональних даних, що містяться в Директиві, і, таким чином, розширює сферу дії законодавства ЄС про захист персональних даних.

Відповідно до GDPR, онлайн-ідентифікатори та інформація, пов'язана з цими онлайн-ідентифікаторами, часто є персональними даними. Якщо зібрана інформація є псевдонімізованою, вона вважатиметься персональними даними, і псевдонімізація буде діяти як запобіжний захід, приноситиме користь суб'єкту даних і виключатиме дані з певних зобов'язань GDPR.

Типи псевдонімізованих даних, які зазвичай використовуються компаніями в сфері онлайн-реклами, такі як ідентифікатори реклами пристроїв та ідентифікатори cookie, зазвичай (залежно від конкретної ситуації компанії, яка обробляє дані) підпадають під категорію персональних даних і, таким чином, підпадають під вимоги GDPR. Компанії у сфері цифрової реклами повинні ретельно вивчити свою діяльність з обробки даних, щоб переконатися, що, якщо вони обробляють персональні дані, то ця обробка відповідає вимогам GDPR.

https://iabeurope.eu/wp-content/uploads/2019/08/20170719-IABEU-GIG-Working-Paper02_Personal-Data.pdf

Обробка персональних даних за згодою

Робочий документ №3

Зміст

- Обробка персональних даних на основі згоди
- Згода за GDPR
- Коли потрібна згода?
- Розкриття відповідної інформації на запит про отримання згоди
- Згода як умова доступу до послуги/Деталізація згоди
- Сфера застосування згоди
- Запис згоди для убезпечення її дотримання Право на відкликання згоди
- Обов'язки першої та третьої осіб
- Заяви або поведінка, що кваліфікуються як згода
- Отримання дійсної згоди на практиці
- Спадкова згода: Дійсність згоди, отриманої до прийняття GDPR
- Згода дітей віком до 16 років
- Резюме

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Обробка персональних даних на основі "Згоди"

"Згода" відповідно до GDPR

"Згода" відповідно до GDPR є набагато більш опрацьованним та коректним поняттям, ніж "згода" відповідно до попередньо існуючого тлумачення **Директиви**. На відміну від Директиви, GDPR чітко та зрозуміло описує вимоги до "згоди", ефективно припиняючи певні трактування та реалізації на практиці "згоди" на підставі старого законодавства. Зокрема це стосується певних понять "припущеної згоди", за якими користувач вважався згодним з запитом шляхом бездіяльності, оскільки згідно з GDPR для "згоди" потрібен прояв чіткої стверджувальної дії.

"Згода" визначена у статті 4(11) GDPR:
Згода суб'єкта даних означає будь-яке вільно надане, конкретне, поінформоване та однозначне зазначення бажань суб'єкта даних, яким він або вона, шляхом оформлення заяви чи проявом чітких ствердних дій, підтверджує згоду на опрацювання своїх персональних даних.

На додаток до "звичайної згоди", яка визначена вище, GDPR також вводить другий тип "згоди": "явну згоду". "Явна згода" не визначена у GDPR, але, як правило, вона трактується як вищий стандарт з деякими більш жорсткими вимогами, наприклад, вимагає більш явного прояву чіткої стверджувальної дії або заяви, яку суб'єкт даних повинен зробити для демонстрації та надання "явної згоди". У ситуаціях, коли необхідна "згода", GDPR зазвичай вимагає "звичайну згоду", в той час як "явна згода" має більш обмежене застосування.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Коли Потрібна Згода? (1/2)

Організації, які бажають обробляти персональні дані, повинні обґрунтовувати необхідність їхньої обробки згідно з законодавством ЄС. GDPR пропонує шість правових підстав для досягнення цього, з яких принаймні одна повинна застосовуватися. "Згода" суб'єкта даних на обробку його персональних даних, є однією з таких правових підстав.

Слід зауважити, що всі правові підстави мають рівну вагу, і жодна з них не має переважного статусу. Вибір найбільш відповідної правової підстави для обробки персональних даних компанії повинен базуватися на контекстуальній оцінці, враховуючи всі відповідні правила, визначені в GDPR та іншому законодавстві.

GDPR визначає певні спеціальні категорії персональних даних, які не можуть бути оброблені, якщо не виконуються більш жорсткі вимоги, що містяться у Статті 9(2), такі як "явна згода" суб'єкта даних: дані, що розкривають расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, чи членство в професійних спілках, і обробка генетичних даних, біометричних даних для цілі єдиної ідентифікації фізичної особи, даних стосовно стану здоров'я чи даних про статеве життя фізичної особи чи її сексуальної орієнтації.

Крім того, певні типи обробки персональних даних підлягають більш жорстким вимогам, наприклад, передача персональних даних за межі території ЄС до країн, які не визнані такими, що забезпечують належний рівень захисту персональних даних, або прийняття рішень, що базуються виключно на автоматизованій обробці та можуть мати юридичні або інші значущі наслідки.

Компанії, які бажають обробляти спеціальні категорії персональних даних або займатися конкретними регульованими видами обробки, повинні дотримуватися більш жорстких вимог щодо обробки.
Крім того, інше законодавство може впливати на рішення щодо вибору найбільш відповідної або необхідної правової підстави для обробки. Зокрема, так зване "положення про файли cookie" **e-Privacy Директиви** визначає:
«…зберігання інформації або отримання доступу до вже збереженої інформації на кінцевому обладнанні абонента або користувача дозволяється лише за умови, що відповідний абонент або користувач дав свою "згоду", отримавши чітку та повну інформацію відповідно до законодавства Європейського Союзу та держав-членів, зокрема щодо мети обробки…"

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Коли Потрібна Згода? (2/2)

Стаття 95 GDPR щодо взаємозв'язку між GDPR та e-Privacy Директивою встановлює, що правила e-Privacy Директиви про обробку даних у сфері послуг електронного зв'язку переважають над загальними правилами GDPR.

Отже, компанії, які зберігають інформацію (наприклад, у файлах cookie) або отримують доступ до інформації (наприклад, ідентифікатори пристроїв, такі як AAID, IDFA або статистичні ідентифікатори, створені за допомогою методів відбитків пальців), повинні враховувати відповідне національне законодавство, що реалізує e-Privacy Директиву, при виборі відповідної законної підстави для обробки зібраних даних.

Компанії також повинні слідкувати за поточними обговореннями **щодо e-Privacy Регламенту,** який передбачає заміну та зміну правил існуючої e-Privacy Директиви.

В той час як директива (наприклад, e-Privacy Директива) зазвичай повинна бути інтрегрована в національне законодавство окремих держав-членів, перш ніж вона створить правові зобов'язання для компаній, регламент (наприклад, GDPR та запропонований e-Privacy Регламент) застосовується безпосередньо в усьому Європейському Союзі без необхідності його інтеграції в національне законодавство держав-членів.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Розкриття необхідної інформації на запит про отримання згоди (1/2)

Згідно з GDPR, суб'єкт даних повинен бути проінформований принаймні про дані контролера та про цілі обробки персональних даних.

Крім того, згода повинна бути зрозумілою, чітко та точно вказувати на обсяг та наслідки обробки персональних даних.

Згідно з Статтею 29 Робочої Групи*: "На практиці це означає, що згода суб'єкта даних повинна ґрунтуватися на розумінні фактів і наслідків тієї чи іншої дії. Зацікавленій особі повинна бути надана в чіткій і зрозумілій формі точна і повна інформація з усіх відповідних питань".

Отже, для того, щоб бути дійсними, запити на згоду та інформація повинні:

(1) бути доступними та розміщуватися окремо від іншої інформації про умови та положення користування відповідним сайтом або сервісом;
(2) бути викладені просто та зрозуміло;
(3) описувати характер оброблюваних персональних даних (наприклад, випадкові ідентифікатори, дані про перегляд);
(4) описувати цілі обробки;
(5) пояснювати наслідки (якщо є такі) обробки;
(6) надавати інформацію про контролера/контролерів, які будуть використовувати згоду для обробки персональних даних (окремо за їхніми найменуваннями);
(7) інформувати користувачів про їх право відкликати згоду, а також про способи відкликати згоду**.

Коментар юриста:
**Варто зауважити, що станом на 2023 Робоча Група змінена на European Data Protection Board – Європейську раду із захисту даних*
***Існував також пункт 8 «навчати користувачів про наслідки відмови у наданні згоди на обробку, наприклад, зменшеного користувацького досвіду або обмеження доступу до сайту чи сервісу» , проте станом на серпень 2023 він становить порушення чинного законодавства.*

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Розкриття необхідної інформації на запит про отримання згоди (2/2)

Згідно з GDPR, немає вимоги, щоб у запитах про згоду перелічувалися найменування операторів, які будуть обробляти дані від імені контролера. Оператор може здійснити обробку на підставі отриманої згоди та наданих інструкцій від свого кнтролера.

Через великий обсяг вимог щодо розкриття інформації, передбачених GDPR, які роблять неможливим або неефективним надання всіх деталей одночасно, IAB Europe рекомендує використовувати "послідовний підхід" для розкриття всієї відповідної інформації. За словами ICO, органу із захисту даних у Великій Британії, послідовні підходи працюють "дуже добре" у онлайн-контексті, наприклад, в контексті цифрової реклами.

"Послідовний підхід може бути корисним, оскільки він дозволяє негайно надати основну **приватну (конфіденційну)** інформацію, і при цьому мати більш деталізовану інформацію доступною в інших джерелах для тих, хто бажає її отримати. Це використовується у випадках, коли унеможливлюється надання деталізованої інформації, або якщо потрібно пояснити особливо складну інформаційну систему користувачам.

Зазвичай розкриття інформації складається з короткого повідомлення, що містить основну інформацію, таку як ідентифікація організації та спосіб використання особистої інформації. Розкриття інформації може містити посилання, що розширюють кожний розділ до повної версії або одне посилання на друге, більш широке повідомлення, яке надає більш детальну інформацію. Таке повідомлення, в свою чергу, може містити посилання на додатковий матеріал, який пояснює конкретні питання, наприклад, такі як умови розкриття інформації поліції".

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Згода як Умова для Отримання Доступу до Сервісу

При визначенні того, чи є "згода" наданою вільно, GDPR вимагає "найпильнішої уваги" до того, чи залежить надання сервісу від отримання "згоди" на обробку даних, яка не є необхідною для надання сервісу.

Стаття 43 описує цю вимогу наступним чином:

"Згода вважається не наданою вільно, якщо [...] виконання контракту, включаючи надання послуги, залежить від "згоди", незважаючи на те, що така "згода" не є необхідною для такого виконання".

Важливо зауважити, що GDPR не забороняє умову доступу до сервісу за допомогою "згоди", хоча вимагає оцінки контексту. E-Privacy Директива роз'яснює, що доступ до "вмісту веб-сайту все ще може бути обумовлений детально осмисленою "згодою" на використання файлів "cookies" та використання подібних технологій відстеження.

В результаті цифрові сервіси, такі як веб-сайти або додатки, зазвичай можуть вимагати від користувачів "згоду" на збір їх персональних даних за допомогою файлів "cookies" або подібних технологій перед наданням доступу до сервісу, при цьому надаючи користувачу можливість ознайомитись із змістом ресерсу.

Коментар юриста:
*Відповідно до GDPR згода має бути надана «вільно». Згода не повинна розглядатися як добровільна, якщо суб'єкт даних не має **справжнього** чи **вільного** вибору **або не може** відмовитися чи відкликати згоду без шкоди для себе.*
*Слід розрізняти так звані "необхідні файли cookie" ("necessary cookies") для функціонування веб-сайту та інші файли cookie (маркетингові файли cookie, файли cookie продуктивності тощо). Що стосується необхідних файлів cookie, то згода користувача не потрібна, оскільки основа легітимізації ґрунтується на необхідності мати можливість керувати вашим веб-сайтом, це файли cookie, без яких неможливо отримати доступ до вмісту веб-сайту. Для всіх інших типів файлів cookie **необхідно отримати інформовану згоду користувача**, а також дозволити користувачеві легко змінити свою згоду в майбутньому.*

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Згода як Умова для Отримання Доступу до Сервісу

10 квітня 2018 року Робоча група зі статті 29 (попередня назва EDPB) прийняла Керівні принципи щодо згоди відповідно до GDPR. 4 травня 2020 року EDPB надала оновлену версію відповідних настанов.

Основні положення:

- відповідно до GDPR згода має бути надана «вільно». Згода не повинна розглядатися як добровільна, якщо суб'єкт даних не має справжнього чи вільного вибору або не може відмовитися чи відкликати згоду без шкоди для себе;
- GDPR передбачає, що «заява або чітка позитивна дія» є необхідною умовою для «звичайної» згоди. Оскільки вимога щодо «звичайної» згоди в GDPR вже підвищена до вищого стандарту порівняно з вимогою щодо згоди в Директиві, необхідно уточнити, яких додаткових зусиль повинен вжити контролер, щоб отримати чітку згоду суб'єкта даних відповідно до GDPR;
- «стіни файлів cookie» ("Cookiewalls") – не є дійсною згодою, оскільки надання послуги залежить від натискання суб'єктом даних кнопки «Прийняти файли cookie». Така дія фактично не є справжнім вибором суб'єкта даних;
- прокрутка всього сайту не означає, що користувач надав свою згоду на використання своїх даних для цілей прямого маркетингу. Особливо тому, що з огляду на GDPR згода вимагає чіткої та позитивної дії.

Отже, якщо компанія хоче обробляти персональні дані своїх користувачів для цілей, які не відповідають початковій меті, для якої дані були спочатку зібрані, компанія зобов'язана отримати попередню та активну згоду суб'єкта даних для цієї конкретної мети. Це можливо, наприклад, за допомогою чек боксів.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Згода як Умова для Отримання Доступу до Сервісу

Крім того, в дизайні cookie банерів, що розміщуються на сайті, потрібно уникати так званих “dark patterns”:

- **Попередньо позначені поля:** веб-сайти не можуть використовувати попередньо проставлені чек бокси для отримання згоди користувача, оскільки вони не є вільним вибором, і користувач не здійснює жодних стверджувальних дій, щоб дати згоду в таких випадках.
- **Згода під час прокручування**: продовження перегляду веб-сайту або бездіяльність щодо банера cookie не може вважатися згодою, наданою користувачем, і не є дійсною відповідно до GDPR.
- **Банер лише для сповіщень**: банери, які не дають користувачам можливості приймати та відхиляти файли cookie, не можуть бути засобом отримання дійсної згоди за GDPR, якщо ваш веб-сайт не використовує лише суворо необхідні файли cookie.
- **Відсутність кнопки «Відхилити»**: банери файлів cookie мають надавати користувачам можливість відхиляти файли cookie, а відхилити згоду має бути так само легко, як надати її.
- **Комплексна згода**: згода на файли cookie не може поєднуватися з іншими положеннями та умовами чи повідомленнями про конфіденційність. Ви також повинні надати користувачам можливість давати згоду на використання різних категорій файлів cookie.
- **Незрозуміла мова**: ви не можете використовувати подвійні заперечення та заплутану мову, щоб спонукати користувачів приймати файли cookie. Використання файлів cookie має бути чітко вказано простою мовою.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Деталізація згоди

Для того, щоб згода була обґрунтованою та проінформованою, цілі обробки даних повинні бути повністю розкриті. Крім того, для того, щоб згода була надана вільно, суб'єкт даних повинен мати можливість окремо надавати згоду на різні операції з обробки персональних даних. Контролер має дозволити користувачам окремо погоджуватися на різні цілі обробки даних, надаючи їм можливість більш усвідомленого вибору.

Вирішення питання щодо відповідності деталізації повинно здійснюватися видавцями на підставі їхнього досвіду роботи зі своїми сервісами та доступами, що стосуються того, які цілі обробки даних є відповідними умовами для доступу до сервісу або які цілі обробки даних є необхідними для забезпечення певного користувацького досвіду. Якщо одна ціль обробки даних залежить від іншої, не можна надавати згоду на першу без згоди на другу. Наприклад, реклама на основі інтересів може залежати від аналітики для вимірювання ефективності реклами. Тому користувач, який не надав згоду на аналітику, не повинен отримувати рекламу на основі інтересів, тому що це взаємозалежно.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Межі Застосування Згоди

Згода може бути отримана першою особою зі свого боку або від третіх особ - партнерів (чи партнерів партнерів) на сервісно-специфічній або глобальній основі. Сервісно-специфічна згода описує наявність або відсутність згоди для певного контролера, який обмежений лише одним сайтом або сервісом, тоді як глобальна згода описує наявність або відсутність згоди для певного контролера без обмежень, де цю згоду можна використовувати.

Згідно зі Статтею 29 Робоча група підтримує принцип глобальної згоди на підставі того, що це забезпечить кращий досвід для користувача. Зокрема, за їхньою думкою, для звичайного користувача кількість запитів на згоду з часом зменшується, коли користувач переміщується та виражає свою згоду в Інтернеті, оскільки: "[...] якщо рекламна мережа третьої особи на веб-сайті отримує згоду на використання файлу "**OBA (Opting Out of Online Behavioral Advertising) cookie**", ця згода буде чинною не тільки на інших сторінках того самого веб-сайту, але й для інших веб-сайтів, які спільно використовують цю ж **OBA (Opting Out of Online Behavioral Advertising)** рекламну мережу".

Компанії повинні впевнитися, що вони знають, який тип згоди (тобто глобальну чи сервісно-специфічну) вони отримали через підрядника (тобто першу особу), оскільки це визначає обсяг дозволеного збору та обробки даних. З цією метою треті особи, які покладаються на згоду користувача, отриману за їхньою допомогою від перших осіб, повинні розглянути контрактні умови та/або інші механізми, включаючи технічні механізми, що відображають обсяг (наприклад, "глобальний") та цілі (наприклад, "реклама на основі інтересів"), які переслідує третя особа.

GDPR не містить строку дії згоди. Отже, згода є чинною, доки обробка персональних даних необхідна для досягнення її цілі або поки суб'єкт даних не відкликав згоду. В будь-якому випадку рішення про строк дії згоди повинно ґрунтуватися на контекстно-специфічній оцінці з урахуванням всіх відповідних факторів, таких як характер та тривалість обробки.

Робоча група рекомендує переглядати та оновлювати згоду через відповідні проміжки часу в рамках дотримання належної практики обробки та збору даних. Також можуть існувати інші закони, правила або норми, які визначають необхідність оновлення згоди. Наприклад, французький орган з захисту даних (CNIL) вважає, що трекінгові cookies можуть зберігатися протягом 13 місяців перед тим, як вони повинні видалятися, що потребує від контролерів отримання згоди користувача на зберігання або доступ до cookies на їхньому пристрої принаймні кожні 13 місяців.[29] Тому компанії повинні враховувати всі відповідні фактори при визначенні того, як часто оновлювати згоду, і чи потрібно взагалі. Однак контролер може потребувати запиту згоди від певного користувача раніше, якщо контролер не може підтвердити, що користувач вже надав таку згоду до цього.

Реєстрація Згоди для Демонстрування Виконання Вимог

Згідно з GDPR контролери повинні "бути здатні продемонструвати, що суб'єкт даних дав згоду на обробку своїх персональних даних".[30] Це означає, що всі контролери (перші та треті особи) повинні вести записи про те, на що окрема особа дала згоду, включаючи мову, яка була використана в механізмі згоди, а також коли та як особа надала згоду.

У випадках, коли контролер обробляє дані на підставі згоди, отриманої від іншої компанії (особи), контролер повинен отримати та зберігати запис, який підтверджує та демонструє, що згода дійсно була отримана, щоб виконати це зобов'язання. З цієї причини важливо, щоб згода користувача передавалася від першої особи всім відповідним третім особам для того, щоб кожна особа могла зберігати задокументований ланцюжок для перевірки наявності згоди аудиторами. IAB Europe рекомендує впроваджувати автоматизований механізм, який передає відповідну інформацію через ланцюжок постачання цифрової реклами.

Такі записи повинні містити, щонайменше:

- Дату та час, коли користувач надав згоду;
- URL-адресу, для якої користувач надав згоду;
- Дію, яку користувач здійснив, щоб надати згоду;
- Цілі, для яких користувач надав згоду;
- Контролер або контролери, або оператори та додаткові оператори (суб-оператори), для яких користувач надав згоду;
- Інформацію, яка була надана користувачу до надання згоди;
- Ідентифікатор, що дозволяє контролеру пов'язати окрему згоду з відповідним користувачем.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Право на відкликання згоди

Суб'єкти даних також мають право відкликати свою згоду у будь-який час, що в першу чергу має бути так само легко зробити, як і надати її.[31] Коли суб’єкт даних відкликає свою згоду, це не впливає на законність обробки, яка відбувалася на підставі цієї згоди до її відкликання.

Однак будь-яка майбутня законна обробка даних, які вже були зібрані або будуть зібрані в майбутньому, вимагатиме іншої юридичної підстави для обробки.

Крім того, якщо користувач відкликає свою згоду на певну діяльність з обробки даних, і не існує іншої юридичної підстави для продовження обробки, користувач має право вимагати видалення (або анонімізації) персональних даних, що його стосуються.

Коли Контролер отримує запит на видалення персональних даних, він повинен виконати запит "без необґрунтованої затримки", за винятком випадків коли ці дані необхідні:
(a) для реалізації права на свободу вияву поглядів та свободу інформації;
(b) для дотримання встановленого законом зобов'язання, що вимагає обробки згідно з законодавством ЄС або держави-члена, яке поширюється на контролера, або для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера;
(c) на підставах суспільного інтересу в сфері охорони суспільного здоров'я;
(d) для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей, мірою, якою видалення даних ймовірно унеможливить або серйозно обмежить досягнення цілей такого опрацювання; або
(e) для формування, здійснення або захисту правових претензій.

На завершення, контролери, які розкрили персональні дані іншим контролерам, повинні вжити "раціональних заходів" для передачі запиту суб'єкта на видалення цих персональних даних іншим контролерам.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Відповідальність Першої та Третьої осіб

Перші особи часто виступають єдиними суб'єктами в ланцюгу цифрової реклами, які можуть надавати інформацію користувачам та отримувати їхню згоду.

Це означає, що перші особи повинні здійснювати необхідне інформування про обробку персональних даних, яка відбувається в результаті доступу користувача до їхнього сайту, додатку або іншої послуги, та запитувати згоду користувача як на обробку персональних даних, за яку вони відповідають, так і на обробку персональних даних, яку здійснюють треті особи.

Однак, навіть якщо треті особи не можуть інформувати та отримувати згоду самостійно, вони можуть бути відповідальними, якщо надане першою особою інформування та отримані згоди юридично недійсні та призводять до невиконання третьою особою вимог законодавства[37].

Тому надзвичайно важливо, щоб екосистема цифрової реклами тісно співпрацювала для виконання обов'язків окремих компаній щодо здійснення відповідного інформування та отримання юридично дійсної згоди відповідно до GDPR.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Заяви або поведінка, що кваліфікуються як чітка стверджувальна Згода

У Статті 29 Робоча група заявила, що "[в принципі] не існує обмежень, що стосуються форми, яку може мати згода [за винятком того, що] вона повинна бути активно виражена.
Пояснювальна частина статті 32 GDPR наводить приклади того, що має, і не має означати "чітка стверджувальна дія":
"Це може включати активацію чекбоксу при відвідуванні Інтернет-сайту, вибір технічних налаштувань у сфері суспільних інформаційних послуг або інші заяви або дії, які чітко свідчать про згоду суб'єкта даних щодо запропонованої обробки його персональних даних. Тому попередньо активовані чекбокси або бездіяльність не є наданням згоди."

Внаслідок впровадження e-Privacy Директиви, отримання згоди на збір персональних даних за допомогою файлів "cookies“, призначених для надання послуг з онлайн-реклами та аналітики в багатьох країнах-членах ЄС зосередилося навколо так званих "банерів згоди", тобто, банерів, розташованих у верхній або нижній частині веб-сторінки, що містять інформацію про цілі збирання даних та запит на згоду.

«Банер згоди» на використання файлів cookie повинен з'явитися, щойно користувач заходить на сайт. Сайт не повинен використовувати файли cookie, доки користувачі не вирішать прийняти, заборонити або налаштувати різні трекери.

На відміну від стіни з файлами cookie, банери з файлами cookie надають користувачам три опції:
- Прийняти всі файли cookie
- Заборонити всі файли cookie
- Налаштувати файли cookie

Відповідно до GDPR, ви повинні надавати своїм користувачам інформацію про:
- Як ви використовуєте файли cookie
- Чому ви їх збираєте
- З ким ви ділитеся інформацією
- Як ваші користувачі можуть відкликати згоду в будь-який час

Щоб згода на файли cookie була дійсною відповідно до GDPR, вона має:
- Вільно надаватися — користувач повинен мати справжній вибір прийняти або відхилити файли cookie.
- Бути конкретною та поінформованою — ви повинні пояснити використання файлів cookie, цілі, з якими вони використовуються, і як користувач може відкликати згоду в будь-який час.
- Бути однозначною та стверджувальною — згода має бути надана чіткою та позитивною дією, наприклад натисканням кнопки «Погоджуюсь».

Заяви або поведінка, що кваліфікуються як чітка стверджувальна Згода

На відміну від Директиви, GDPR чітко передбачає, що обробка будь-яких персональних даних не може починатися до моменту настання дії, якою користувач продемонстрував надання згоди на таку обробку.

Згідно з GDPR, користувач не може бути примушений надавати згоду, що по суті робить consent wall. В 2020 році* EDPB випустило гайд про те, що використання consent wall є недопустимим: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Прокрутка сторінки не є наданням згоди станом на 2023*.

Процес, за допомогою якого користувачі можуть надавати згоду на використання файлів cookie, повинен передбачати позитивну дію або іншу активну поведінку, за умови, що вони були повністю проінформовані про те, що ця дія означає. Тому користувачі можуть надавати свою згоду, натискаючи кнопку або позначаючи чекбокс у полі поряд з місцем, де представлена інформація про збір їхніх персональних даних (якщо дія виконується разом із наданою інформацією про використання файлів cookie), або будь-якою іншою активною поведінкою, з якої адміністратор веб-сайту може однозначно зробити висновок про конкретну та проінформовану згоду."

**До 2020 року застосовувався підхід, що оскільки обробка за згодою користувача, така як збір даних за допомогою файлів “cookies”, не може починатися до конклюдентної чіткої ствердної дії, перші сторони особи можуть захотіти замість цього показати проміжний сайт, що запитує згоду. Такі проміжні сайти називаються "стіна згоди" ("consent wall"). Це гарантуватиме, що користувачі прочитали та погодилися з обробкою, необхідною для надання послуги, перед її використанням. Хоча згода також може бути виражена через дію подальшого використання послуги після належного інформування, наприклад, за допомогою "банера згоди", важливо, щоб збір та обробка даних не відбувалися до моменту однозначної конклюдентної чіткої ствердної дії, що означає надання згоди у:*

***Раніше Стаття 29 Робочої групи визначала "активну поведінку" як дію користувача, "засновану на відстежуванному запиті користувача-клієнта до веб-сайту". Крім того, Робоча група вважала, що "дія користувача повинна бути такою, що, у поєднанні із наданою інформацією про використання файлів cookie вона може бути аргументовано інтерпретована як ознака його/її бажань." Французький орган з захисту даних також зазначав, що згода "може бути виражена прокруткою відвідуваної веб-сторінки».*

Отримання чіткої стверджувальної Згоди на практиці

Протокол прозорості та згоди IAB Europe («**IAB Europe TCF**» або «**Протокол**») має просту мету - допомогти всім сторонам ланцюга цифрової реклами виконувати вимоги GDPR та e-Privacy Директиви щодо обробки персональних даних, доступу та/або зберігання інформації на пристрої користувача, такої як файли cookie, ідентифікатори реклами, ідентифікатори пристрою та інші технології відстеження.

Протокол особливо важливий для перших осіб, таких як видавці та інші постачальники онлайн-послуг, які співпрацюють з третіми особами для здійснення обслуговування на основі даних.

Використовуючи Протокол, перші особи можуть дозволити третім особам обробляти дані користувачів на основі однієї із правових підстав регулювання.

Протокол стандартизує представлення запитів третіх сторін користувачам, які потребують проінформованої згоди на обробку персональних даних.

Протокол дозволяє "сигналізувати" вибір користувача всьому ланцюгу рекламного постачання. Він є відкритим джерелом і не приносить прибутку, а управління ним засноване на консенсусі в галузі, визначеному на чолі з IAB Europe, із значною підтримкою з боку інших сторін у галузі та IAB Tech Lab, яка забезпечує технічне управління відкритими специфікаціями та контроль версій.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Згода дітей молодше 16 років

У випадку, коли інтернет-послуга надається безпосередньо дитині, згода є юридичною підставою для обробки лише у випадку, якщо дитина досягла принаймні 16 років; якщо дитина молодша 16-ти, необхідна згода її законного представника.

Держави-члени можуть прийняти законодавство, що знижує цей поріг, за умови, що нижній вік не буде меншим за 13 років.

У разі потреби в згоді законного представника дитини контролери також повинні вжити розумних заходів для підтвердження такої згоди.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Резюме

- Згода є однією з шести правових підстав для обробки персональних даних згідно з GDPR. Вибір відповідної правової підстави для обґрунтування обробки персональних даних вимагає аналізу конкретного контексту. Одними із важливих контекстуальних факторів виступають інші закони, такі як ePrivacy Директива, яка вимагає згоду на зберігання або доступ до інформації, збереженої на пристроях кінцевих користувачів.

- Обробка даних на основі згоди не може розпочинатися до вчинення активної, чіткої та стверджувальної дії суб'єктом даних.*

- При отриманні згоди важливо, щоб суб'єктам даних була надана правильна інформація, включаючи деталі, такі як цілі обробки даних, типи даних, які будуть оброблятися, відповідальні контролери та інше. Для кожної мети обробки має бути окремо надана згода. Користувач має розуміти, на що конкретно він погоджується. Оскільки це великий обсяг інформації, ми рекомендуємо використовувати багаторівневий підхід, де ключова інформація надається спочатку, з посиланням на більш детальну інформацію.

- Перші особи перебувають у найкращому положенні для надання інформації користувачам та отримання згоди, тому відповідальність за необхідні розкриття інформації та отримання згоди часто лежить на них. Треті особи також несуть відповідальність за коректне отримання згоди з їхнього боку.

- Забороняється вимагати згоду та робити доступ до сайту/сервісу залежним від наявності згоди** Про це свідчать як роз'яснення EDPB, так і відповідні висновки регуляторних органів європейських країн, зокрема, в площині неправомірності застосування «стін файлів cookie» ("cookie walls") та вимог до оформлення банерів згоди, що розміщуються на сайтах перших осіб та їхніх партнерів.

- Згода має бути деталізованою з точки зору цілей обробки, для яких суб'єкт даних надає згоду Якщо компанія хоче обробляти персональні дані своїх користувачів для цілей, які не відповідають початковій меті, для якої дані були спочатку зібрані, компанія зобов'язана отримати попередню та активну згоду суб'єкта даних для цієї конкретної мети. Це можливо, наприклад, за допомогою чек боксів. Водночас, згода на файли cookie не може поєднуватися з іншими положеннями та умовами чи повідомленнями про конфіденційність. Користувачам має бути надна можливість давати згоду на використання різних категорій файлів cookie.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Резюме

- Згода має бути деталізованою з точки зору цілей обробки, для яких суб'єкт даних надає згоду Якщо компанія хоче обробляти персональні дані своїх користувачів для цілей, які не відповідають початковій меті, для якої дані були спочатку зібрані, компанія зобов'язана отримати попередню та активну згоду суб'єкта даних для цієї конкретної мети. Це можливо, наприклад, за допомогою чек боксів. Водночас, згода на файли cookie не може поєднуватися з іншими положеннями та умовами чи повідомленнями про конфіденційність. Користувачам має бути надна можливість давати згоду на використання різних категорій файлів cookie.

- Згода може бути специфічною для конкретної послуги або загальною, що означає, що згода дійсна на різних веб-сайтах та послугах для того самого Контролера. Перші особи визначають обсяг згоди, яку вони запитують. Згоду можуть отримувати перші особи від імені третіх осіб, з якими вони співпрацюють.

- Контролери повинні зберігати записи про отримання згоди. IAB Europe рекомендує впровадження автоматизованого механізму, який передає відповідну інформацію через ланцюжок постачання цифрової реклами (supply chain).

- Згоду має бути так само легко відкликати, як і надавати. Обробка персональних даних, що відбувається до відкликання, залишається законною. Персональні дані, зібрані до відкликання згоди, не можуть оброблятися після відкликання, якщо немає альтернативної правової підстави для обробки цих даних.

- Група з реалізації GDPR у IAB Europe розробляє технічний стандарт для спрощення обміну інформацією між першими та третіми особами, що може допомогти в розкритті інформації, створенні записів про отримання згоди та передачі цієї інформації по ланцюжку постачання цифрової реклами.

**Багато поточних методів отримання згоди не є достатніми для доведення, що користувачі вчинили "Конклюдентну дію", щоб вказати свою "згоду". На відміну минулого ставлення до цього питання, обробка даних на основі "згоди" не може розпочинатися до отримання "згоди" конклюдентно.*

*** Раніше приватним компаніям дозволялося зробити доступ до своїх послуг залежним від "згоди" суб'єктів даних. GDPR передбачає врахування цього при визначенні, чи була "згода" надана добровільно, але не забороняє таку практику. Крім того, e-Privacy Директива також пояснює, що послуги можуть бути залежними від "згоди".*

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180907_IABEU-GIG_Working-Paper03_Consent_v1.1.pdf

Запити суб'єктів даних

Робочий документ №4

Зміст

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Запити від суб'єктів даних (1/2)

У порівнянні із попереднім законодавством ЄС, GDPR розширив наявні права у сфері даних, що надаються суб'єктам даних відповідно до законодавства ЄС про захист даних, як зазначено у Главі III GDPR «Права суб'єкта даних». Він також встановлює додаткові права стосовно «персональних даних», що збираються контролерами або під їхнім керівництвом.

Ці дані, своєю чергою, можуть оброблятися постачальниками послуг або операторами. Залежно від обставин суб'єкти даних можуть вимагати перегляд своїх даних, які зберігаються контролером, вимагати виправлення чи видалення даних, просити контролера припинити чи обмежити обробку персональних даних та/або запитати перенесення персональних даних до іншого постачальника послуг.

Внаслідок цих змін виникла низка відкритих питань щодо того, як цих прав у сфері персональних даних дотримуються в цифровому маркетингу. Зокрема, дотримання права суб'єктів даних є складним процесом, оскільки компанії цифрового маркетингу традиційно зберігають дані під псевдонімами та не завжди мають безпосередні відносини з окремими особами. Наприклад, точкою взаємодії для персональних даних може бути щось дуже просте — ідентифікатор cookie або ідентифікатор мобільного пристрою.

Мета цього документа — надати учасникам сфери цифрового маркетингу, зокрема компаніям у сфері рекламних технологій, аналіз цих прав і краще розуміння варіантів реагування на можливі ситуації звернень суб'єктів даних. Цей документ також надає компаніям основні рекомендації щодо виконання правил, які вони зможуть переглянути зі своїми юристами, щоб зрозуміти, як правильно дотримуватися прав суб'єктів даних.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Запити від суб'єктів даних (2/2)

Важливо підкреслити, що кожна технологічна платформа в секторі цифрового маркетингу є унікальною та надає різноманітні послуги своїм клієнтам. Отже, кожна компанія впроваджуватиме процеси та процедури, які є специфічними для цієї компанії, що призведе до різних реакцій на зобов’язання щодо дотримання та реалізації прав суб'єктів даних. Цей документ має на меті надати загальні вказівки, думки та варіанти щодо того, як дотримуватись прав суб'єктів даних і реагувати на запити щодо них. Компанії повинні переглянути ці вказівки, оскільки вони стосуються їхніх унікальних систем, зі своїм юрисконсультом.

Крім того, у цей документ включена рекомендація компаніям брати до уваги інші практики захисту персональних даних, оприлюднені відповідно до GDPR. Наприклад, принцип мінімізації даних вимагає, щоб організації обробляли персональні дані лише в обсязі, необхідному для досягнення цілей обробки. Компанії можуть розглянути можливість подальших кроків щодо псевдонімізації чи агрегації даних або навіть кроків щодо видалення даних для дотримання прав суб'єктів даних. Знову ж таки, не всі компанії можуть вживати тих самих заходів щодо мінімізації даних, псевдонімізації, агрегації даних або видалення даних, які вживають інші компанії.

Цей документ може бути оновлено, оскільки регулятивні органи надають додаткові вказівки, або завдяки відгукам членів IAB Europe.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Крок 1: Оператор і контролер

Один з перших кроків, яких мають вжити організації в екосистемі цифрової реклами для дотримання цих прав — переглянути сам текст GDPR і переконатися, що вони розуміють, як ці права впливають саме на їхні послуги та процеси. Зокрема, компанії у сфері цифрового маркетингу спочатку повинні визначити, чи вони є контролером (в тому числі, спільним чи незалежним), чи оператором, щоб з'ясувати, яка сторона має реагувати на запит суб'єкта даних.

На всі організації, які діють як контролери, може з високою ймовірністю безпосередньо впливати необхідність дотримання права суб'єктів даних. Своєю чергою, оператори можуть допомагати контролерам дотримуватися цих прав суб'єктів даних. Наприклад, операторам може бути потрібно впровадити технологічні зміни, які сприятимуть виконанню контролером зобов’язань з реагування на запити щодо дотримання права суб'єктів даних відповідно до GDPR.

Оператори даних не повинні безпосередньо відповідати на запити щодо доступу, якщо інше не зазначено в угоді з контролером чи в інших документах. Контролери повинні чітко вказати роль кожної сторони щодо дотримання прав суб'єктів даних у своєму контракті чи в угоді/додатку про обробку даних. Якщо контролер не надав відповідної інструкції, оператори не можуть безпосередньо відповідати за запит щодо доступу з боку суб'єкта даних або розголошувати інформацію суб'єкта даних без вказівки контролера. Це може вважатися порушенням безпеки персональних даних, що включає «несанкціоноване розкриття […] персональних даних», хоча ризик мінімальний, оскільки дані псевдонімізовані (див. визначення нижче). Крім того, якщо оператор починає відповідати на запити щодо прав суб'єкта даних без вказівок чи без інформування контролера, такий оператор наражається на ризик бути визнаним організацією-контролером."

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Крок 2: Виняток із прав суб’єктів даних (2/3)

Другий крок — визначити, чи компанії у сфері цифрового маркетингу становлять один з винятків, що стосуються реагування на запити щодо прав суб'єктів даних. Згідно зі статтею 11, якщо персональні дані, які опрацьовує контролер, не надають йому можливості ідентифікувати фізичну особу, контролер даних не повинен бути зобов’язаним отримувати додаткову інформацію для того, щоб ідентифікувати суб'єкта даних, винятково для цілей дотримання GDPR.
Стаття 12 GDPR також зазначає, що контролер може відмовити «від дій на запит суб'єкта даних щодо реалізації його прав за статтями 15–22», якщо контролер продемонструє неможливість ідентифікувати суб'єкта даних.

Згідно зі статтею 11 GDPR, якщо цілі, для яких контролер обробляє персональні дані, не вимагають або більше не вимагають ідентифікації суб'єкта даних контролером, контролер не зобов’язаний зберігати, отримувати або обробляти додаткову інформацію для ідентифікації суб'єкта даних для єдиною метою дотримання цього Регламенту. Якщо у випадках, зазначених у частині 1 цієї статті, контролер може продемонструвати, що він не в змLIA ідентифікувати суб’єкта даних, контролер повинен повідомити про це суб’єкта даних, якщо це можливо. У таких випадках статті з 15 по 20 не застосовуються, за винятком випадків, коли суб’єкт даних, з метою здійснення своїх прав згідно з цими статтями, надає додаткову інформацію, що дозволяє його або її ідентифікацію.

Більшість компаній у сфері цифрового маркетингу збирають, обробляють і передають псевдонімізовані дані, тобто персональні дані, які не можуть бути віднесені до конкретного суб'єкта даних без використання додаткової інформації. Така додаткова інформація може зберігатися окремо, «і на неї поширюється застосування технічних і організаційних інструментів для забезпечення того, що персональні дані не віднесено до фізичної особи, яку ідентифіковано чи можна ідентифікувати».

Наприклад, компанії у сфері цифрового маркетингу зазвичай збирають і обробляють ідентифікатори, такі як ідентифікатори файлів cookie або ідентифікатори мобільного пристрою, або іншу інформацію під псевдонімами, ідентифікуючи браузер або пристрій, а не особу. Вони не збирають, не отримують і не зберігають персональну інформацію, таку як ім'я «Джон Сміт».

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Крок 2: Виняток із прав суб’єктів даних (2/3)

"Щоб належним чином відповісти на запит суб'єкта даних, компаніям у сфері цифрового маркетингу доведеться отримати додаткову інформацію від сторонньої компанії, такої як постачальник, або від самого суб’єкта даних, щоб ідентифікувати та підтвердити конкретну особу на основі ідентифікатора cookie або ідентифікатора мобільного пристрою, який вони зберігають. Ці додаткові дані були б необхідні для фактичної ідентифікації особи. У наведеному вище прикладі, якщо особа надсилає своє ім’я, наприклад, Джон Сміт, рекламній компанії, ця компанія не має такої персональної інформації без псевдонімів у своїй системі, щоб надати інформацію, пов’язану з іменем особи. У цьому прикладі контролер повинен отримати та обробити додаткову інформацію від стороннього постачальника, щоб ідентифікувати суб'єкта даних виключно з метою дотримання GDPR.

"Ще більше занепокоєння викликає запитання, як компанії зі сфери цифрового маркетингу, які використовують псевдонімізовані дані, взагалі можуть підтвердити, що дані належать особі, яка їх запитує?

Вони не в змLIA безпосередньо ідентифікувати суб’єкта даних, а персональні дані не можна віднести до конкретного суб’єкта даних. Не маючи ані імені, ані адреси особи, як компанії цифрового маркетингу можуть підтвердити, що файл cookie або ідентифікатор мобільного пристрою пов’язаний з браузером або мобільними програмами, які належать особі, яка надсилає запит суб’єкта даних, навіть якщо ця особа надає своє ім’я та адресу?

Навіть маючи ім'я та адресу, компанії зі сфери цифрового маркетингу не можуть пов'язати цю інформацію з псевдонімізованими даними у своїй системі. Наприклад, чоловік-кривдник може надіслати компанії ідентифікатор cookie з ноутбука своєї дружини з проханням надати доступ до даних, пов’язаних із цим ідентифікатором cookie.

Компанія не має можливості перевірити, чи ідентифікатор cookie або ідентифікатор мобільного пристрою належить чоловікові чи дружині.

Дії компанії можуть призвести до витоку особистих даних через випадкове або «несанкціоноване розкриття або доступ до» персональних даних однієї особи іншій особі.

Компанії зі сфери цифрового маркетингу майже не мають варіантів дійсно перевірити, що саме ця особа — власник ідентифікатора cookie або іншого ідентифікатора, наприклад ідентифікатора мобільного пристрою. Відповідаючи на такий запит, компанія могла б, наприклад, надіслати цьому чоловікові історію вебперегляду дружини."

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Крок 2: Виняток із прав суб’єктів даних (3/3)

"Враховуючи нездатність перевірити, чи дані, щодо яких надійшов запит, належать особі, яка цей запит подає, виникає ключове запитання: чи мають компанії зі сфери цифрового маркетингу, які збирають тільки псевдонімізовані дані, відповідати на запити суб'єктів даних?

Компаніям потрібно оцінити, чи варто реагувати на запити суб'єктів даних у кожному конкретному випадку, і зафіксувати ці міркування. Цей аналіз має вирішальне значення, оскільки європейські регулятори зайняли різні позиції щодо реагування на запити суб'єктів даних.

Наприклад, британський регулятор (ICO), схоже, підтримує думку про те, що на запити доступу від суб'єкта (SAR) потрібно відповідати у всіх можливих випадках. Як зазначено в «Практичному кодексі доступу суб’єктів» ICO: «[Закон про захист даних] покладає на вас високі вимоги щодо надання інформації у відповідь на запити доступу від суб'єкта».

З іншого боку, німецькі регуляторні органи висловлюють застереження у своєму короткому документі про права суб'єктів даних, рекомендуючи компаніям враховувати інші права та свободи, такі як права інтелектуальної власності та таємниці компанії. Інші органи захисту персональних даних рекомендували, що якщо компанія не може встановити особу, яка подає запит, вона може розглянути можливість надання особі інформації про те, як компанія сегментує аудиторію, але не зобов’язана надавати особі інформацію, до якого саме сегменту належить ця особа.

Компаніям варто переглянути варіанти відповіді на запити суб'єктів даних зі своїм юристом з питань зовнішньої взаємодії та визначити, чи варто взагалі відповідати на кожен окремий запит. Після прийняття рішення ми наполегливо рекомендуємо компаніям створити внутрішню політику реагування на запити суб'єктів даних, яка б також покривала всі взаємодії з запитами суб'єктів даних на доступ, особливо причини відмови у виконанні такого запиту.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Крок 3: Політика

Якщо компанія приймає рішення, що вона зобов'язана реагувати на запити суб'єктів даних, ми рекомендуємо, щоб така компанія створила внутрішню письмову політику, яка визначала б процедури відповіді на запити доступу до даних. Наприклад, у цій політиці має бути визначено, які ідентифікатори суб'єктів даних (наприклад, ідентифікатори файлів cookie або мобільні рекламні ідентифікатори) необхідно надати, і яка інформація про суб'єкта даних необхідна для підтвердження особи, а також описана процедура відповіді на такі запити, яка діє в компанії.

З точки зору процедури, компанії повинні чітко вказати в письмовій формі, що вони готові розглянути запит, вказати процес перевірки або іншого підтвердження автентичності власності на браузер або пристрій, увімкнути пошук за ідентифікатором суб'єкта даних і надати можливість знаходити, переглядати та видаляти дані за потреби.

У політиці також має бути визначено період збереження запитів суб'єкта даних і відповідей компанії. Іншими словами, якщо суб'єкт даних подає запит 1 січня 2023 року, як довго компанія зберігатиме листування між суб’єктом персональних даних і компанією та (якщо такі є) будь-які результати запиту? Компаніям не потрібно відповідати на запити суб'єктів даних, які стосуються даних, які вони видалили, деідентифікували або анонімізували, що відповідно виводить їх за межі GDPR.

Таким чином, компаніям слід розглянути можливість впровадження надійної політики збереження даних не лише для забезпечення дотримання GDPR, але й для того, щоб допомогти обмежити обсяг відповідей щодо запитів доступу від суб'єктів даних.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Конкретні права суб’єктів даних

Інформація

Контролери даних повинні прозоро доносити суб'єктам даних інформацію щодо обробки їх персональних даних. Такі повідомлення мають надаватися у стислому, прозорому, зрозумілому та легкодоступному вигляді, чіткою простою мовою. Контролер повинен надати суб'єкту даних інформацію, викладену в главі III, розділі 2, статті 13-14 GDPR.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Стаття 13. Інформація, яку необхідно надати у разі збирання персональних даних від суб'єкта даних

1. Якщо персональні дані щодо суб’єкта даних збирають від суб’єкта даних, контролер повинен, у момент отримання персональних даних, надати суб’єкту даних усю інформацію, а саме інформацію про:

(a) особу та контактні дані контролера та, за необхідності, представника контролера;

(b) контактні дані співробітника з питань захисту даних, за необхідності;

(c) цілі опрацювання, для досягнення яких призначено персональні дані, а також законодавчу базу для опрацювання;

(d) якщо опрацювання здійснюють на підставі пункту (f) статті 6(1), законні інтереси контролера або третьої сторони;

(e) одержувачі чи категорії одержувачів персональних даних, за наявності;

(f) за необхідності, інформацію про те, що контролер має намір передати персональні дані до третьої країни чи міжнародної організації, про наявність чи відсутність рішення Комісії про відповідність, або, у випадку актів передавання, вказаних у статті 46 чи 47, або другому підпараграфі статті 49(1), – зазначення належних чи відповідних гарантій і засобів, за допомогою яких можна отримати копію таких даних, або джерела, звідки їх можна отримати у вільному доступі.

Стаття 13. Інформація, яку необхідно надати у разі збирання персональних даних від суб'єкта даних

2. Крім інформації, вказаної в параграфі 1, контролер повинен, у момент отримання персональних даних, надати суб'єкту даних усю детальну інформацію, необхідну для забезпечення правомірного та прозорого опрацювання, а саме інформацію про:

(a) період зберігання персональних даних, або, якщо це неможливо, – критерії визначення такого періоду;

(b) існування права на запит від контролера щодо доступу до персональних даних і їх виправлення, стирання, обмеження опрацювання щодо суб'єкта даних або на заперечення проти опрацювання, а також права на мобільність даних;

(c) якщо опрацювання здійснюють на підставі пункту (a) статті 6(1) або пункту (a) статті 9(2), – існування права на відкликання згоди в будь-який момент, без наслідків для законності опрацювання, що було засновано на згоді до її відкликання;

(d) право подавати скаргу до наглядового органу;

(e) те, чи є надання персональних даних статутною чи договірною вимогою, або вимогою, необхідною для укладення контракту, а також – чи зобов'язаний суб'єкт даних надати персональні дані, та про можливі наслідки ненадання таких даних;

(f) наявність автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу, вказаного в статті 22(1) та (4) і, принаймні в таких випадках, достовірної інформації про логіку, значимість та передбачувані наслідки такого опрацювання для суб'єкта даних.

3. Якщо контролер прагне надалі опрацьовувати персональні дані для іншої цілі, ніж та, для якої персональні дані було отримано, контролер повинен надати суб'єкту даних до початку такого подальшого опрацювання інформацію про таку іншу ціль і будь-яку належну детальну інформацію, як вказано в параграфі 2.

4. Параграфи 1, 2 і 3 не застосовують, якщо і оскільки суб'єкт даних уже володіє інформацією.

Стаття 14. Інформація, яку необхідно надати у разі отримання персональних даних не від суб'єкта даних

1. Якщо персональні дані було отримано не від суб’єкта даних, контролер повинен надати суб’єкту даних інформацію, а саме про:

(a) особу та контактні дані контролера та, за необхідності, представника контролера;

(b) контактні дані співробітника з питань захисту даних, за необхідності;

(c) цілі опрацювання, для досягнення яких призначено персональні дані, а також законодавчу базу для опрацювання;

(d) категорії відповідних персональних даних;

(e) одержувачі чи категорії одержувачів персональних даних, за наявності;

(f) за необхідності, про те, що контролер прагне передати персональні дані до одержувача в третій країні чи міжнародної організації, про наявність чи відсутність рішення Комісії про відповідність, або, у випадку актів передавання, вказаних у статті 46 чи 47, або другому підпараграфі статті 49(1), – зазначення належних чи відповідних гарантій і засобів, за допомогою яких можна отримати копію таких даних, або джерела, звідки їх можна отримати у вільному доступі.

Стаття 14. Інформація, яку необхідно надати у разі отримання персональних даних не від суб'єкта даних

2. Крім інформації, зазначеної в параграфі 1, контролер повинен надати суб'єкту даних інформацію, необхідну для забезпечення правомірного та прозорого опрацювання, що стосується суб'єкта даних, а саме про:

(a) період зберігання персональних даних, або, якщо це неможливо, – критерії визначення такого періоду;

(b) якщо опрацювання здійснюють на підставі пункту (f) статті 6(1), законні інтереси контролера або третьої сторони;

(c) існування права на запит від контролера щодо доступу до персональних даних і їх виправлення, стирання, обмеження опрацювання щодо суб'єкта даних і на заперечення опрацювання, а також права на мобільність даних;

(d) якщо опрацювання здійснюють на підставі пункту (a) статті 6(1) або пункту (a) статті 9(2), – існування права на відкликання згоди в будь-який момент, без наслідків для законності опрацювання, що ґрунтувалося на згоді до її відкликання;

(e) право подавати скаргу до наглядового органу;

(f) те, з якого джерела походять персональні дані, та, за необхідності, про те, чи надійшли вони з джерел, доступних для громадськості;

(g) наявність автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу, вказаного в статті 22(1) та (4) і, принаймні в таких випадках, достовірної інформації про логіку, значимість та передбачувані наслідки такого опрацювання для суб'єкта даних.

3. Контролер повинен надати інформацію, вказану в параграфах 1 та 2:

(a) у розумний строк після отримання персональних даних, але щонайменше протягом одного місяця, враховуючи конкретні обставини, за яких опрацьовують персональні дані;

(b) якщо персональні дані необхідно використати для спілкування з суб'єктом даних, – принаймні в момент першого повідомлення такому суб'єкту даних; або,

(c) якщо передбачається розкриття іншому одержувачу, – принаймні під час першого розкриття персональних даних.

Стаття 14. Інформація, яку необхідно надати у разі отримання персональних даних не від суб'єкта даних

4. Якщо контролер прагне надалі опрацьовувати персональні дані для іншої цілі, ніж та, для якої персональні дані було отримано, контролер повинен надати суб'єкту даних до початку такого подальшого опрацювання інформацію про таку іншу ціль і будь-яку належну детальну інформацію, як вказано в параграфі 2.

5. Параграфи 1 – 4 не застосовують, якщо і оскільки:

(a) суб'єкт даних уже володіє інформацією;

(b) надання такої інформації стає неможливим чи викликало б несумісні наслідки, зокрема, для опрацювання задля досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілях, із урахуванням умов і гарантій, зазначених у статті 89(1) або доки обов'язок, вказаний у параграфі 1 цієї статті, ймовірно унеможливить або серйозно обмежить досягнення цілей такого опрацювання. У таких ситуаціях контролер повинен вжити необхідних заходів для захисту прав і свобод та законних інтересів суб'єкта даних, у тому числі, оприлюднення інформації;

(c) отримання чи розкриття прямо передбачено законодавством Союзу або держави-члена, яке поширюється на контролера та яким передбачено необхідні заходи для захисту законних інтересів суб'єкта даних; або

(d) якщо персональні дані необхідно залишати в таємниці відповідно до обов'язку збереження професійної таємниці, що регулюється законодавством Союзу або держави-члена, в тому числі, статутний обов'язок збереження таємниці.

Електронна пошта або веб-сайт

Компанії повинні, як мінімум, оприлюднити адресу електронної пошти, яку особи можуть використовувати для надсилання запитів щодо своїх прав.

Ця адреса електронної пошти може бути обліковим записом, який використовується для зв’язку з відповідальною особою компанії з питань захисту персональних даних.

Компанії повинні розглянути можливість вжити заходів для забезпечення ретельного моніторингу облікового запису електронної пошти, включно з ситуаціями, коли одержувач або відповідальна особа, яка відповідає на такі запити, перебуває у відпустці або припиняє працювати в компанії.

Компанія також може розглянути можливість додати CAPTCHA або інший механізм, щоб переконатися, що запит надходить від реальної особи (наприклад, privacy@company.com можна записати як Privacy AT Company .com).

У компанії також може бути окрема сторінка на веб-сайті, в якій роз'яснюються процедури відповіді на запити суб'єктів даних з питань їхніх прав. (Див. рекомендовані кроки для перевірки інформації про суб’єкта даних нижче). Принаймні одна особа має нести відповідальність за відповіді на запити суб'єктів даних, надіслані через веб-сайт, поштою, електронною поштою чи сторінки компанії у соцмережах.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Право доступу

Відповідно до GDPR суб'єкти даних мають право запитувати контролера даних, чи обробляє він їхні персональні дані. За певними винятками, на запит суб'єкта даних щодо реалізації його прав контролер повинен надати такому суб'єкту даних наступну інформацію, яка може бути включена до повідомлення про приватність (конфіденційність) або іншого загальнодоступного документа компанії:

1. чи обробляються персональні дані суб'єкта;
2. цілі обробки;
3. категорії даних, що обробляються;
4. категорії одержувачів, яким можуть передаватися дані, зокрема одержувачі в третіх країнах (країни, що не входять до ЄС) або міжнародні організації;
5. період зберігання даних;
6. право суб'єкта даних вимагати виправлення або видалення персональних даних, а також право обмежувати обробку персональних даних чи відмовитися від неї;
7. право подати скаргу до наглядового органу;
8. інформація щодо джерела даних, якщо дані не були отримані безпосередньо від суб'єкта даних;
9. інформація щодо застосування будь-якої автоматизованої обробки персональних даних суб'єктів даних, включно з профілюванням, згаданим у статті 22(1) і (4) GDPR, що здійснює правовий або інший значущий вплив на суб'єкта даних, а також параметри таких автоматизованих рішень; і
10. копія персональних даних, що обробляються (за запитом).

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Право на виправлення

Враховуючи цілі обробки, особи мають право вимагати від контролера виправити будь-які помилки в записах їхніх персональних даних. Такі виправлення можуть включати доповнення неповних персональних даних, якщо це доцільно, за допомогою додаткової заяви. Компанії повинні створити політику для процесу виправлення, яка повинна включати перевірку особи суб'єкта даних перед внесенням будь-яких змін.

Певні компанії, які сегментують аудиторію (наприклад, відвідувачі веб-сайту, які цікавляться темою «взуття»), можуть налаштувати сегмент аудиторії суб'єкта даних відповідно до запиту суб'єкта даних (наприклад, змінити категорію суб'єкта даних із «Потенційно відвідує Францію» на «Любить проводити час вдома»). Отримані зміни можуть не відображатися, доки компанія сфери цифрового маркетингу не стикнеться з тим самим суб'єктом даних на іншому веб-сайті.

Беручи до уваги принципи мінімізації даних, альтернативна позиція полягає в тому, що компанії цифрового маркетингу можуть запровадити свою політику та процедури щодо права на видалення (див. «Право на видалення» нижче). Уточнимо: компанії цифрового маркетингу можуть бути не в змLIA виправити необроблені дані, що лежать в основі їхніх сегментів аудиторії, як-от записані базові URL-адреси чи розташування мобільних пристроїв. Ці логи є просто записам про сайти чи програми чи широту/довготу, які відвідав суб'єкт даних, або це навіть може бути запис, пов'язаний із самою рекламою, а не з особистими даними особи (наприклад, оголошення було доставлено на сайт у певний час дня, особа натиснула на нього тощо). Ці параметри є точним відображенням даних, зібраних компаніями сфери цифрового маркетингу.

Компанії сфери цифрового маркетингу можуть дозволити людям виправити сегменти аудиторії, до яких вони належать. Однак багато компаній сфери цифрового маркетингу створюють сегменти аудиторії на основі алгоритмів, і виправлення таких сегментів може конфліктувати з цим алгоритмом. Крім того, компанії цифрового маркетингу можуть вважати виправлення даних надзвичайно складним або майже неможливим, оскільки це може вимагати від компаній отримання та виправлення інформації в різних базах даних. Таким чином, видалення даних у відповідь на такий запит може бути простішим рішенням для суб'єкта даних, оскільки він більше не буде «помилково» пов'язаний із певним сегментом аудиторії.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Право на видалення (1/2)

Суб’єкти даних мають право на видалення даних, яке вимагає від контролера видалення усіх збережених персональних даних, що стосуються особи, без «необґрунтованої затримки», якщо застосовується одна з наступних умов:

1) «персональні дані більше не є необхідними для виконання цілей, для яких вони були зібрані або іншим чином оброблені». Вищезазначена умова означає, що компанії сфери цифрового маркетингу повинні переглянути та створити загальну політику щодо того, чи потрібно їм зберігати певні дані для цілей, для яких вони були спочатку зібрані чи оброблені, наприклад виставлення рахунків, запобігання шахрайству чи з інших причин безпеки. Якщо компанія вирішує не видаляти певні дані, вона повинна чітко зафіксувати таке рішення та потреби в продовженні обробки, оскільки органи захисту даних, ймовірно, використовуватимуть дуже вузьке тлумачення того, коли справді необхідно зберігати дані.

2) «суб’єкт даних відкликає згоду, на якій ґрунтується обробка, згідно з пунктом (a) статті 6(1) чи пунктом (a) статті 9(2), та якщо немає іншої законної підстави для обробки». Це положення стосується тих компаній сфери цифрового маркетингу, які є контролерами та покладаються на згоду як правову основу для обробки персональних даних суб’єкта даних, і суб’єкти даних згодом відкликають свою згоду. Персональні дані видаляються, коли суб’єкт даних відкликає свою згоду. Контролери також повинні перевірити, чи існує інша правова підстава для обробки даних (наприклад, законний інтерес, такий як збереження даних для виставлення рахунків, щоб запобігти шахрайству).

3) «суб’єкт даних заперечує проти обробки згідно зі статтею 21(1), та немає жодних першочергових законних підстав для обробки, або суб’єкт даних заперечує проти обробки згідно зі статтею 21(2)». Це положення застосовується до тих компаній сфери цифрового маркетингу, які є контролерами, покладаючись на законний інтерес як правову основу для обробки персональних даних суб’єкта даних. Якщо суб’єкт даних заперечує проти обробки, «на підставах, пов’язаних із його чи її конкретною ситуацією», а також просить видалити персональні дані, контролер, який покладається на законний інтерес, може відхилити цей запит, якщо доведе, що його інтереси переважають права особи. Компанії можуть стверджувати, що інтереси запобігання шахрайству, надання послуг безпеки чи збереження даних для фінансових записів чи звірки можуть переважати над правами особи. Знову ж таки, компанії повинні фіксувати свою логіку, якщо вирішать, що їм потрібно зберігати певні дані.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Право на видалення (2/2)

4) «персональні дані обробляються незаконно». Це положення застосовується, коли основоположна законність обробки поставлена під сумнів і, отже, вважається незаконною. Персональні дані обробляються незаконно, якщо правова основа для оброблення недійсна або не існує, а також якщо обробка не відповідає принципам обробки даних за GDPR. Якщо правова основа для обробки є незаконною, компанія цифрового маркетингу повинна буде видалити дані за запитом суб'єкта даних. GIG IAB Europe пояснює, що компанії можуть виконувати цю вимогу шляхом видалення або хешування (без можливості виділення браузера чи пристрою) ідентифікатора файлів cookie (без можливості розшифрувати хешовану інформацію, включаючи знищення ключа), мобільного ідентифікатора чи іншого ідентифікатора, який використовується для поєднання даних рівня користувача з ідентифікатором. Ідентифікатор потрібно або видалити, або хешувати в базі даних компанії сфери цифрового маркетингу. Потім компанія також може або видалити файл cookie у веб-браузері особи, або змінити термін дії існуючого файлу cookie на пристрої особи. Компанія також може повідомити суб’єктам даних, як вони можуть видалити свої файли cookie за допомогою елементів керування браузера.

У випадку мобільних додатків особі слід порадити скинути мобільний рекламний ідентифікатор. У будь-якому випадку ідентифікатор пристрою стає анонімним лише тоді, коли він хешується на стороні сервера (стороні компанії) ТА видаляється на стороні суб’єкта даних. Усунувши ідентифікатори (та/або можливість визначити особу), пов’язані з даними, або скинувши мобільний ідентифікатор, компанія фактично pLIAрве зв’язок між персональними даними та особою, яку можна ідентифікувати, що призведе до того, що компанія більше не матиме персональних даних — навіть псевдонімізованих. Натомість компанія зберігатиме анонімні дані, які не підпадають під дію GDPR. Це тлумачення повністю покладається на здатність компанії довести, що немає способу пов’язати зібрані дані з будь-якою особою, а також не матиме змоги інакше поводитися з цією конкретною особою (або з пристроєм, який органи захисту даних за наближенням ототожнюють з особою).

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Право на обмеження обробки (1/2)

Право на обмеження обробки персональних даних є новим правом суб'єкта даних. Суб'єкти даних можуть обмежити цілі, для яких контролер може обробляти їхні дані. Це проміжний крок, менш радикальний, ніж видалення, який особи можуть вимагати, коли вони заперечують проти певних способів обробки їхніх даних (наприклад, для судових позовів). Суб'єкти даних мають право вимагати обмеження обробки персональних даних, якщо застосовується одна з таких умов:

1. Суб'єкт даних оскаржує точність персональних даних, протягом періоду часу, що надає контролеру можливість перевірити точність персональних даних;
2. Обробка є незаконною, але суб'єкт даних виступає проти видалення персональних даних і натомість надсилає запит на обмеження їх використання;
3. Контролеру більше не потрібні персональні дані для цілей обробки, але їх вимагає суб'єкт даних для формування, здійснення або захисту правових претензій
4. Суб'єкт даних заперечив проти обробки згідно зі статтею 21(1) в очікуванні проведення перевірки щодо того, чи переважають законні підстави контролера над законними інтересами суб'єкта даних.

У результаті запровадження цього права контролери даних повинні забезпечити можливість «зупинити» або призупинити обробку будь-яких даних з обмеженим доступом. Наприклад, компанія цифрового маркетингу може зробити вибрані дані недоступними для подальшої обробки або позначити дані на серверах, щоб автоматично виключити їх з обробки. Організації можуть розглянути можливість переміщення обмежених даних до іншої системи даних, щоб запобігти обробці. Ця вимога також може бути виконана за допомогою надання суб'єктам даних можливості відмовитися від обробки даних іншим чином. Компанія сфери цифрового маркетингу може скинути файл cookie для відмови у веб-браузері користувача або еквівалентний ідентифікатор мобільного пристрою для відмови, щоб компанія більше не збирала жодних даних, навіть для вимірювання, показу реклами чи звітності. Це позначило б веб-браузер або мобільний пристрій особи як обмежений і заборонило б подальшу обробку даних.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Право на обмеження обробки (2/2)

У своїй відповіді на запит суб’єкта даних компанія повинна повідомити суб’єкта даних, що навіть якщо його дані обмежені та більше не оброблятимуться активно, вони все одно можуть зберігатися. Внутрішньо організація також може визначити, чи є у неї підстави наполягати на обробці даних, незважаючи на запит (наприклад, якщо організація має підтвердження згоди суб’єкта даних). Якщо контролер за контрактом розкрив персональні дані третій особі, і дані суб’єкта з тих пір були обмежені, контролер повинен повідомити таких третіх осіб про всі зміни. Контролер також повинен поінформувати про цих отримувачів суб'єкта даних за запитом останнього.

Якщо контролер може довести, що виконання цього зобов’язання є неможливим або вимагатиме непропорційних зусиль, тоді існує виняток для цього зобов’язання повідомляти суб’єкта даних і третіх осіб-партнерів згідно зі статтею 19. Персональні дані можуть не обмежуватися та оброблятися повторно, коли застосовується одна з наступних умов:

1. якщо фізична особа надала згоду — вона має бути поінформована про те, що компанія сфери цифрового маркетингу знову обробляє персональні дані;
2. для здійснення або захисту правових вимог;
3. для захисту прав іншої особи чи організації; або
4. з міркувань важливого суспільного інтересу ЄС або країни ЄС.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Право на перенесення даних (1/2)

Право на перенесення даних також є новим правом суб'єкта даних, яке вимагає більше зусиль, ніж інші права доступу до даних.

1. Суб'єкти даних мають право отримати персональні дані, які вони надали контролеру даних, якщо: a) обробка ґрунтується на згоді або на основі договору, та b) обробка здійснюється автоматизованими засобами.
2. Суб'єкт даних має право отримати свої персональні дані «у структурованому, широко вживаному форматі, який легко зчитується машиною, та передавати ці дані іншому контролеру».
3. Завдяки цьому праву особа може вимагати від контролера перенести або передати дані іншому контролеру.

Права на перенесення даних активуються лише в обмеженому наборі обставин.

По-перше, як зазначалося вище, це право застосовується, лише якщо особа надає дані контролеру. Окремі особи не завжди надають дані контролерам в екосистемі цифрового маркетингу. Наприклад, компанії сфери цифрового маркетингу збирають дані осіб, коли вони відвідують цифрові ресурси, такі як веб-сайти та мобільні додатки. Перенесення даних стосується лише даних, які були безпосередньо надані контролеру відповідною особою, а не даних, створених компанією або наданих компанії іншими особами. Це не стосується, наприклад:

1. Даних, наданих іншими особами про цю особу;
2. Даних, створених контролером; і
3. Даних, отриманих контролером на основі обробки інших даних

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Право на перенесення даних (2/2)

Таким чином, термін «надані» включає персональні дані, які стосуються діяльності суб'єкта даних або є результатом спостереження за поведінкою особи, але не застосовується до будь-якого подальшого аналізу чи висновків щодо цієї поведінки. Робоча група погодилася з цим аналізом, зазначивши у своїх рекомендаціях, що йдеться про дані, «надані» суб'єктом даних, включаючи «історію використання веб-сайту», але не подальші дані, створені контролером, такі як профіль користувача. Будь-які персональні дані, які були згенеровані контролером даних у рамках обробки даних (наприклад, у процесі персоналізації чи рекомендацій, категоризації чи профілювання користувачів), є даними, які отримані або випливають із персональних даних, наданих суб'єктом даних, і на них не поширюється право на перенесення даних.

По-друге, права на перенесення даних можуть бути активовані, якщо правова основа для збору персональних даних ґрунтується на згоді, явно вираженій згоді, або для виконання контракту. Це право не застосовується, якщо обробка ґрунтується на інших правових підставах, ніж згода особи або виконання контракту.

Нарешті, право на перенесення даних не може негативно впливати на права та свободи інших (наприклад, якщо йдеться про більше ніж одну особу). Якщо компанії цифрового маркетингу не можуть підтвердити, що ідентифікатор належить суб'єкту даних, виконання запиту на перенесення даних може призвести до передачі даних неправильному одержувачу, що негативно вплине на права та свободи справжнього суб'єкта даних. Потенційно це також може становити порушення безпеки персональних даних, хоча шкода мінімізована, оскільки компанії цифрового маркетингу, ймовірно, збирають і зберігають дані під псевдонімом. Тому компанії повинні бути обережними, відповідаючи на запити щодо перенесення даних. Знову ж таки, якщо компанія сфери цифрового маркетингу вважає, що не може передати персональні дані, які вона зібрала, іншій компанії внаслідок цієї проблеми, вона повинна задокументувати свої аргументи.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Право на заперечення

Коли дані обробляються на підставі законного інтересу, суб’єкти даних мають право «заперечувати» щодо обробки своїх персональних даних, якщо дані використовуються для цілей маркетингу даних або профілювання або обробляються для дослідницьких чи статистичних цілей. Це означає, що право на заперечення згідно зі статтею 21(2) виходить за рамки не лише надання реклами особі, але й заборони подальшого профілювання для цілей прямого маркетингу.

Якщо обробка базується на правовій основі «законний інтерес», компанії сфери цифрового маркетингу повинні використовувати повідомлення про конфіденційність (приватність), щоб поінформувати суб'єктів даних, що вони мають право заперечити щодо збору даних відразу ж або ж якнайшвидше по тому. Це право має бути окремим положенням у повідомленні про конфіденційність (приватність). В ідеалі компанії повинні надати засоби для надсилання запитів в електронному вигляді, бажано в автоматизований спосіб заперечення, тобто надати посилання для відмови. Якщо компанії сфери цифрового маркетингу є операторами даних, їм слід розглянути можливість надання контролерам даних можливості керувати різними списками відмови для цілі обробки даних.

Під час розробки політики стосовно права суб’єкта даних на заперечення організації повинні враховувати такі моменти:

1. Що відбувається, коли суб'єкт даних бажає «заперечити»?
2. Які дані збирає організація після активації права на заперечення?

Якщо контролер за контрактом розкрив персональні дані третій особі, а суб’єкт даних заперечив щодо обробки цих даних, тоді контролер повинен повідомити цих третіх осіб про всі зміни.

Якщо контролер може довести, що виконання цього обов’язку є неможливим або вимагало б непропорційних зусиль, тоді для контролера існує виняток відповідно до статті 19

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Копія персональних даних, що обробляються

За запитом суб'єкта даних компанії повинні надати копію персональних даних, які вони обробляють, за деякими конкретними винятками. Важливо розуміти, що набір персональних даних, який розкривається суб’єкту даних, залежить від компанії. Наприклад, вимоги до розкриття інформації відрізнятимуться залежно від того, чи класифікується компанія як оператор чи контролер.

Оператор даних, такий як технологічна платформа, отримуючи прямий запит, не повинен розголошувати дані на рівні контролера, якщо відсутня вказівка контролера це зробити.

Компанії сфери цифрового маркетингу можуть розглянути можливість перевірки того, які дані вони могли б розкрити, отримавши запит, пов'язаний з цифровим ідентифікатором.

Крім того, оскільки компанії практично не мають можливості підтвердити особу запитувача даних, компанії можуть розглянути питання про те, щоб не розголошувати запитувачу необроблені дані (наприклад, історію веб-перегляду чи дані потоку кліків). Може бути достатньо надати суб’єкту даних інформацію про те, до яких сегментів аудиторії він належить. Це пов’язано з тим, що наслідки витоку персональни даних або порушення прав особи на захист даних переважають необхідність розголошення таких необроблених даних запитувачу. Це також може призвести до заподіяння шкоди компанії через розкриття її комерційної таємниці (див. обговорення нижче).

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Автоматизована обробка: Профілювання?

Відповідно до GDPR, компанії також зобов'язані інформувати про існування та параметри будь-якої автоматизованої обробки, включаючи профілювання, що має значний вплив на суб'єктів даних. «Профілювання» визначається як «будь-яка форма автоматизованої обробки персональних даних із оцінюванням персональних аспектів, що стосуються фізичної особи, зокрема для аналізу або передбачення аспектів, що стосуються продуктивності суб'єкта даних на роботі, економічної ситуації, здоров'я, особистих уподобань або інтересів, надійності або поведінки, місцезнаходження або пересування».

Профілювання стає важливим, коли його висновки та категоризація запускають автоматичне прийняття рішень. Робоча група опублікувала вказівки щодо визначення автоматизованого прийняття рішень і профілювання, а також щодо того, які рішення мають юридичний або «подібно значущий» вплив.
«Правові наслідки» — це ті, що мають вплив на законні права особи, наприклад, вплив на правовий статус особи. Крім того, «значущі наслідки» — це наслідки, які еквівалентні або подібні до юридичних наслідків. Робоча група прямо заявила, що типова реклама на основі інтересів не матиме настільки значущого впливу, оскільки малоймовірно, що реклама (яку особа може ігнорувати) матиме юридичний або значущий вплив на суб'єктів даних .

Проте Робоча група надала коментарі, щоб допомогти компаніям сфери цифрового маркетингу визначити, чи може їхня бізнес-практика мати значний вплив на особу, наприклад (a) нав'язливість процесу профілювання; (b) очікування та бажання особи; (c) спосіб доставки реклами; та (d) особливу вразливість осіб, яким демонструється відповідна реклама. Наприклад, зазначила Робоча група, різниця в ціні товарів за певних обставин може мати значний вплив на людину.

Компанії сфери цифрового маркетингу, а також веб-сайти та мобільні додатки, які вони підтримують, повинні прозоро розкривати свої бізнес-практики. Як мінімум, вони повинні інформувати, чи на їхньому сайті використовується персоналізована реклама, які технології використовуються для демонстрації цієї реклами, щоб суб'єкт даних міг у будь-який момент від цього відмовитися, а також у який спосіб це можна зробити. Їм також слід переглянути вказівки Робочої групи стосовно того, коли їхні дії можуть розглядатися як «профілювання».

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Перевірка даних (1/4)

Після отримання запиту від суб'єкта даних, компанії повинні вжити розумних заходів, щоб перевірити інформацію про суб'єкта даних, а саме, що запит надійшов від дійсного суб'єкта даних, щоб не довелося обробляти запит, який подала особа, яка не є авторизованим суб'єктом персональних даних, про які йдеться в запиті.
Щоб знизити ризик недоброчесних запитів, компанії повинні перевіряти особу суб'єкта даних, щоб переконатися, що його виконання не буде «негативно впливати на права чи свободи інших осіб». Це особливо важливо для компаній у сфері цифрового маркетингу, які зберігають псевдонімізовані дані.

Це також актуально, коли один браузер або пристрій використовується кількома особами, в результаті чого ідентифікатор cookie призначається кільком особам. Крім того, залишається відкритим питання про те, як відповідати на запити щодо прав суб'єкта даних від представника суб'єкта даних. Як перевірити, що представник має право подавати запити щодо персональних даних від імені особи? Компанії можуть попросити окремих осіб відвідати веб-сайт компанії та заповнити форму, щоб підтвердити свою особу та те, що ідентифікатор пристрою було призначено їхньому пристрою, або отримати доступ до порталу веб-сайту, який підтверджує ідентифікатор пристрою, відповідно до статті 12(6) GDPR.

Тут важливо зазначити, що цей процес перевірки, знов-таки, викликає труднощі для компаній зі сфери цифрового маркетингу. Якщо компанія зберігає непсевдонімізовані персональні дані, наприклад адреси електронної пошти, вона може надіслати посилання для підтвердження на обліковий запис електронної пошти, наданий особою, щоб переконатися, що суб'єкт даних є власником цієї електронної адреси. Однак компанії, які зберігають виключно псевдонімізовані дані, не мають можливості таким чином перевірити особу. Однак, незважаючи на відсутність імені та адреси особи, існує ймовірність того, що компанія цифрового маркетингу не повинна відмовляти в наданні даних суб'єкту даних, а натомість повинна спробувати перевірити право особи на дані, що включає вживання розумних заходів для автентифікації суб'єкта даних.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Перевірка даних (2/4)

Компанії у сфері цифрового маркетингу, які обробляють лише псевдонімізовані дані, повинні відповідати лише на запити суб'єктів даних, пов’язані з ідентифікатором, який вони використовують.

Ці ідентифікатори можуть включати ідентифікатори файлів cookie та ідентифікатори мобільних пристроїв. Якщо суб'єкт даних надсилає своє ім’я, адресу електронної пошти чи IP-адресу, компанії повинні спочатку подати запит на додаткову інформацію від суб'єкта даних. Такі дані можуть включати фактичний файл cookie чи ідентифікатор мобільного пристрою від особи, які компанії з цифрового маркетингу мають право отримувати відповідно до статті 12(6) GDPR. Якщо суб'єкт даних заперечує проти надання запитуваної інформації, компанія може відповісти, що не може виконати запит суб’єкта на доступ без попередньої перевірки того, що особа, яка надсилає запит, має право отримати такі дані.

Крім того, якщо оператор веб-сайту або постачальник мобільного додатка (перша особа) бажає відповісти на запит щодо прав суб'єкта даних, пов’язаний із персональними даними, які зберігаються партнерами з цифрового маркетингу (третя особа), він повинен буде спрямувати суб'єктів даних на сайт партнерів (третьої особи) для виконання такого запиту. Наприклад, якщо особа перейшла на веб-сайт і подала запит на доступ до своїх персональних даних, зібраних партнерами оператора веб-сайту, веб-сайт не зможе зв’язатися зі своїми партнерами, щоб попросити партнера надати такі дані про особу.

Зокрема, сайт не може надсилати ім'я та електронну адресу суб'єкта даних третій стороні, щоб така третя сторона могла знайти інформацію про цю особу, оскільки компанія з цифрового маркетингу не зберігає такі дані, що уможливлюють ідентифікацію. Натомість оператор веб-сайту повинен спрямувати суб'єкта даних на сайт компанії з цифрового маркетингу, де компанія описує, як вона відповідає на запити суб'єктів даних, щоб компанія могла запитати в суб'єкта даних ідентифікатор, який ця особа використовує, і перевірити особу. Знову ж таки, ці ідентифікатори можуть включати ідентифікатори файлів cookie та ідентифікатори мобільних пристроїв.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Перевірка даних (3/4)

Крім того, коли суб'єкт даних надсилає запит і надає ідентифікатор, компанія з цифрового маркетингу може попросити суб'єкта даних надати знімок екрана з ідентифікатором для підтвердження запиту, або ж компанія може створити механізм для автоматичного зчитування файлів cookie з браузера особи.

Якщо необхідно, в електронному листі із запитом на додаткову інформацію компанії зі сфери цифрового маркетингу можуть (1) посилатися на статтю 12(6), (2) пояснювати, як суб'єкти даних можуть знайти свій файл cookie або мобільний ідентифікатор на своїх пристроях, і (3) нагадати суб'єкту даних, що кожен браузер матиме різний набір файлів cookie, і що відповідь суб'єкта даних буде прив’язана до цього конкретного браузера. Знову ж таки, побоювання в цій ситуації викликає те, що якщо суб'єкт даних відмовляється надати запитаний знімок екрана, компанії не зможуть перевірити автентичність запиту.

Крім того, або ж як альтернатива, компанії можуть попросити в суб'єкта даних декларацію чи письмове підтвердження, в якому буде зазначено, що цей суб'єкт даних є власником і користувачем браузера чи мобільного пристрою, і що суб'єкт даних має право подавати запит щодо даних, про які йдеться. Якщо одним пристроєм чи браузером користуються двоє людей, компаніям варто розглянути питання, чи можуть обидві особи підписати підтвердження чи декларацію.

Хоча деякі компанії можуть запитувати копії урядових документів на посвідчення особи від суб'єкта даних, компанії у сфері цифрового маркетингу, які зазвичай не збирають непсевдонімізовані персональні дані, можуть не бажати отримувати та зберігати таку інформацію, через що вони автоматично повинні будуть виконувати суворіші вимоги захисту персональних даних, за допомогою якихі можна ідентифікувати особу. Крім того, немає способу прив'язати ім'я особи, що зазначено на посвідченні особи, з ідентифікатором cookie або іншими цифровими ідентифікаторами, оскільки у світі цифрового маркетингу такі дані рідко пов'язані між собою.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Перевірка даних (4/4)

Знову ж таки, компанії зі сфери цифрового маркетингу можуть пояснити процедури роботи з суб'єктами персональних даних і процес перевірки на окремій сторінці свого веб-сайту. Компаніям також може бути варто використовувати форму для збору інформації, необхідної для обробки запиту від суб'єкта даних. Однак компанії не можуть змусити суб'єкта даних використовувати цю форму. Якщо компанії отримують запит суб'єкта даних через інший канал, наприклад, через електронну пошту чи соціальні мережі, вони повинні направити особу на вебсторінку свого сайту, що стосується прав на персональні дані, або попросити особу зв’язатися з компанією за допомогою призначеної для таких запитів електронної адреси (наприклад, privacy@ company.com).

Підсумуємо: через складність перевірки, що ідентифікатор cookie або мобільного пристрою дійсно належить суб'єкту даних, який подає запит, та через побоювання розкрити персональні дані сторонній особі й таким чином «негативно вплинути на права чи свободи» іншої особи компанії повинні розглянути, які з наступних заходів вони вживатимуть після отримання запиту від суб'єкта даних:

1. Зафіксувати та продемонструвати, що компанія не в змLIA ідентифікувати суб'єкта даних, і поінформувати суб'єкта даних, що відповідь на запит не буде надана;
2. Надати інформацію в повідомленні про конфіденційність або в іншому документі з інструкціями щодо того, як надається відповідь на запити щодо прав суб'єктів даних, включаючи те, що суб'єкт даних повинен надати певну інформацію, таку як знімок екрана з відповідним ідентифікатором і/або з запитом на декларацію чи підтвердження того, що цей ідентифікатор належить відповідному суб'єкту даних, перш ніж компанія зможе відповісти на запит; або
3. Створити вебсторінку, яка дозволить компанії перевірити файли cookie суб'єкта даних у цьому браузері та відповісти на запит суб'єкта даних після перевірки.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Комерційна таємниця

GDPR передбачає, що права доступу будь-якої особи до персональних даних не повинні негативно впливати на права чи свободи компанії чи інших осіб, включаючи комерційні таємниці чи інтелектуальну власність, зокрема програмне забезпечення, яке захищає авторські права.

Логічно, що компанії переймаються потенційним розкриттям комерційних таємниць під час відповіді на запити суб'єктів даних. Зокрема, компанії занепокоєні тим, що зловмисник або конкурент може вирахувати комерційні таємниці з даних, переданих відповідно до запитів на доступ до даних або перенесення даних.

Компанії сфери цифрового маркетингу не повинні надавати дані, які можуть розкрити комерційну таємницю, наприклад, якщо оприлюднення параметрів автоматизованого прийняття рішень передбачає розкриття комерційної таємниці.

Однак, хоча компанії сфери цифрового маркетингу можуть обмежити обсяг оприлюднених даних, якщо таке оприлюднення може завдати шкоди компанії або її інтелектуальній власності, вони не можуть взагалі відмовитися від оприлюднення будь-яких даних. Вони також повинні зафіксувати логіку того, чому оприлюднення такої інформації могло би призвести до розкриття комерційної таємниці.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Відмова

У випадку прийняття рішення про відмову в задоволенні запиту, компанії цифрового маркетингу повинні надати поважну причину для відмови у наданні даних суб'єкту даних.

Наприклад, якщо компанія сфери цифрового маркетингу є оператором або не може достовірно встановити особу запитувача, вона повинна повідомити про цю причину суб'єкта даних. Важливо зазначити, що планка для відмови у праві доступу до даних є високою, про що свідчить справа Доусона-Дамера. (джерело: http://www.bailii.org/ew/cases/EWCA/Civ/2017/74.html) Однак слід зазначити, що справа Доусона-Дамера стосувалась персональних даних, особу суб'єкта яких можна було встановити.

Крім того, як зазначалося раніше, німецькі регулятори запропонували більше свободи для відмов. Компанії сфери цифрового маркетингу також повинні інформувати людей про їхнє право подати скаргу до наглядового органу та звернутися з заявою до суду.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Записи

Компанії сфери цифрового маркетингу повинні вести облік всіх отриманих запитів суб'єктів даних щодо реалізації їх прав і всіх відповідей щодо доступу суб’єктів до даних, які вони надсилають, щоб продемонструвати виконання правил.

Якщо запит надсилається через портал веб-сайту, може бути сенс зберегти певну інформацію для ведення обліку, щоб продемонструвати дотримання права суб'єкта даних на доступ до даних (наприклад, ідентифікатор файлів cookie та мітку часу).

Такий обліковий запис може включати сам запит суб'єкта даних, дату запиту, відповідь компанії (яка може містити відмову), дату відповіді, а також копію ідентифікатора особи, доказ перевірки та інформацію про те, хто обробив запит. Компаніям може знадобитися надати цю інформацію як доказ у разі звернення наглядового органу.

Компанії повинні зберігати записи щодо всієї кореспонденції з відповідними особами протягом встановленого періоду зберігання, що складає принаймні 18-36 місяців.

Члени GIG IAB Europe погодилися, що ці дані можна зберігати довше встановлених стандартних періодів зберігання даних щодо надання послуг компанією, оскільки це окремі дані, які обробляються для різних цілей і на іншій законній підставі (виконання вимог закону).

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Навчання

Компанії сфери цифрового маркетингу повинні навчати своїх працівників відповідати на запити суб'єктів даних відповідно до політики компанії.

Внутрішня політика компанії має бути легко доступною в централізованій локації, наприклад, у внутрішній мережі компанії.

Під час навчання персоналу компанії з питань захисту персональних даних, всіх працівників потрібно навчити ідентифікувати запити від суб'єктів даних відповідно до GDPR, навіть якщо в самих запитах це не зазначено. Наприклад, особа може попросити поінформувати її, які дані зберігає або використовує компанія, не згадуючи GDPR і не позначаючи свій запит як запит суб’єкта даних.

Персонал, який стикається з такими питаннями, має отримати більш ґрунтовне навчання щодо роботи з такими запитами і ситуаціями.

Зокрема, відділ маркетингу, відділ із захисту персональних даних і юридичний відділ потребуватимуть більш конкретизованого навчання, оскільки вони можуть брати більш активну участь в обробці цих запитів. Компанії також повинні забезпечити ієрархію, щоб співробітники могли повідомити про проблему вищому керівництву. Якщо суб'єкт даних буде незадоволений початковою відповіддю щодо доступу до даних, керівник вищої ланки має переглянути відповідь і визначити подальші кроки.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Спосіб передачі даних

Компанії сфери цифрового маркетингу також повинні подбати про метод «передачі» даних та/або надання доступу до них у відповідь на будь-які запити на доступ від суб'єктів даних. GDPR зазначає, що, де це можливо, «контролер повинен бути спроможним надавати віддалений доступ, який забезпечить суб'єкту даних прямий доступ до своїх персональних даних».

Таким чином, компанії сфери цифрового маркетингу можуть розглянути можливість розробки або впровадження систем, які могли б надавати суб'єктам даних віддалений доступ до їх персональних даних, що зберігаються цією компанією, після підтвердження особи. Компанії повинні прагнути надавати дані особам у безпечний спосіб.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Оплата

Згідно зі статтею 12(5) GDPR контролери більше не можуть стягувати розумну плату за відповідь на запити суб’єктів даних. У статті 12(5) зазначено, що «Інформацію, що надають згідно зі статтями 13 і 14, і будь-яке повідомлення та будь-які дії, яких вживають за статтями 15–22 і 34, необхідно надавати на безоплатній основі».

Початкова копія відповіді на запит щодо доступу до даних має бути безкоштовною, але компанії можуть стягувати розумну плату за подальші копії. Наприклад, якщо суб’єкт даних або посередник, що діє від імені суб’єкта даних, робить кілька запитів на доступ до даних, компанії можуть розглянути питання про стягнення розумної плати, виходячи з адміністративних витрат, за будь-які подальші копії, на які подано запит.

Це означає, що з посередника може стягуватися плата, якщо він надсилає численні запити суб’єктів даних від імені різних осіб. Контролер даних в такому випадку має довести, що запит є надмірним і, отже, вимагає оплати. Тому контролер повинен фіксувати кількість запитів від суб'єкта даних, щоб продемонструвати, що такі запити були надмірними та обтяжливими.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Час

Контролер повинен відповідати на запити суб’єктів даних, направлені відповідно до статей 15–22, «без необґрунтованої затримки та протягом одного місяця». Якщо запит надто складний, щоб розглянути його протягом одного місяця, розгляд можна продовжити до трьох місяців.

Однак контролер повинен повідомити суб’єкта даних про будь-яке таке продовження та причину такої затримки протягом одного місяця з моменту отримання запиту.

Контролери повинні пам’ятати, що вони несуть тягар доведення того, що запит є «складним», і компанії сфери цифрового маркетингу повинні задокументувати свої аргументи для висновку, що цей запит вимагає подовження періоду відповіді.

Знову ж таки, компаніям сфери цифрового маркетингу варто розглянути доцільність ведення записів про будь-яку чи всю комунікацію із суб’єктами даних, включаючи спілкування щодо початкового запиту та відповіді на нього. Такі додаткові діалоги між компаніями сфери цифрового маркетингу та суб’єктом даних можуть показати, чому обговорення триває понад один місяць. Якщо так відбудеться, записи компанії зі сфери цифрового маркетингу мають продемонструвати, що компанії потрібна була додаткова необхідна інформація, щоб відповісти на запит суб'єкта даних, і що час на відповідь не збіг, доки компанія не отримала всю необхідну інформацію.

Як зазначалося раніше, листування (і відповіді щодо персональних даних) з кожним суб’єктом даних має зберігатися щонайменше протягом 18-24 місяців.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Зобов'язання повідомляти відповідних третіх осіб

Якщо контролер даних розкриває персональні дані третім особам, а суб’єкт даних згодом здійснює будь-які права на виправлення, видалення чи обмеження, GDPR вимагає від контролера даних інформувати всіх третіх осіб про те, що суб’єкт даних скористався цими правами, якщо тільки зробити це «неможливо або вимагає непропорційних зусиль». За запитом суб’єкта даних контролер також повинен повідомити суб’єкта даних про будь-яких третіх осіб, яким було розкрито його або її персональні дані. Для організацій, які регулярно розкривають персональні дані великій кількості третіх осіб, це може стати особливо обтяжливим.

П’ять кроків, які потрібно зробити відразу ж:

1. Визначте, чи ваша організація є контролером чи оператором;
2. Переконайтеся, що у вас є відповідні процедури та політика для відповіді на запити щодо прав суб’єкта даних, зокрема, коли ви повинні відповідати на такі запити (згода чи законний інтерес) і як ви будете реагувати;
3. Розробіть процес перевірки, щоб переконатися, що суб’єкт даних має право на запитувані персональні дані.
4. Переконайтеся, що ваші співробітники з юридичного відділу, а також відділів маркетингу та безпеки належним чином навчені відповідати на запити суб’єктів даних; і
5. Оновіть свої повідомлення про конфіденційність (приватність), щоб зазначити права суб’єктів даних.

Джерело:https://iabeurope.eu/wp-content/uploads/2019/08/20180406-IABEU-GIG-Working-Paper04_Data-Subject-Requests.pdf

Критерії контролера та оператора

Робочий документ №5

Зміст

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180802_IABEU-GIG-Working-Paper05_Controller-Processor-Criteria.pdf

Ключові терміни

Клієнт / Користувач
Термін «Клієнт» / «Користувач» зазвичай стосується клієнта рекламної платформи.

Суб'єкт даних
GDPR визначає суб'єкта даних як "ідентифіковану фізичну особу" або "фізичну особу, яку можна ідентифікувати". У контексті рекламних компаній, суб'єктами даних зазвичай є користувачі Інтернету, чиї персональні дані збираються та обробляються.

Контролер даних
GDPR визначає контролера даних як фізичну або юридичну особу, державний орган, агентство або інший орган, який самостійно або спільно з іншими визначає цілі та засоби обробки персональних даних. Іншими словами, контролер даних — це суб’єкт, який приймає рішення щодо діяльності з обробки даних, незалежно від того, чи здійснює цей суб'єкт будь-які операції з обробки даних фактично. Важливо відзначити, що конкретні вимоги до контролерів даних і операторів даних можуть бути розглянуті в окремих інструкціях. Як зазначає Робоча Група Статті 29, «контролер може делегувати визначення «засобів» обробки, якщо це стосується технічних або організаційних питань». Однак Робоча група також заявляє, що «визначення «цілі» обробки зберігається за «контролером». Тому той, хто приймає це рішення, є (де-факто) контролером»

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180802_IABEU-GIG-Working-Paper05_Controller-Processor-Criteria.pdf

Ключові терміни

Оператор даних
GDPR термін «Оператор» визначається як фізична або юридична особа, державний орган, агентство або інший орган, який обробляє персональні дані від імені Контролера. Іншими словами, Контролер даних приймає рішення щодо діяльності з обробки даних, Оператор даних - це будь-який суб'єкт, з яким Контролер вступає в угоду для безпосередньо обробки даних. Зазвичай оператор даних не має права використовувати дані, надані Контролером, якщо це не передбачено письмовими вказівками Контролера даних. Операторам все ще можуть надаватись права визначати деякі засоби обробки, якщо це делеговано Контролером, але не "цілі" (згідно зі Статтею 29 Робочої Групи). Тому Оператор може визначати технічні та організаційні заходи для забезпечення обробки даних, якщо вони не є основними елементами процесу обробки. Будь ласка, зверніть увагу, що конкретні вимоги до Контролерів і Операторів даних можуть бути визначені також в окремих інструкціях компетентних органів у сфері захисту даних та приватності.

Суб-оператор
GDPR також регламентує правила для оператора даних, який залучає іншого оператора даних. Останній, у свою чергу, вважається суб-оператором. В контексті рекламних технологій, суб-операторами даних часто є хостингові компанії, сторонні розробники з певним рівнем доступу до персональних даних або інші організації, які надають допомогу оператору даних. Згідно з GDPR, оператор даних повинен отримати дозвіл від контролера даних для призначення суб-операторів даних. Цей дозвіл може бути наданий загальним чином, за умови, що оператор даних інформує контролера даних про всіх суб-операторів, щоб контролер даних мав можливість висловити свої зауваження. Суб-оператори також підпадають під ті ж самі вимоги, що і оператори згідно з GDPR. Це означає, що вони повинні дотримуватися загальних правил і зобов'язань, передбачених регламентом, щодо обробки персональних даних.

Ідентифікатор користувача (англійською «User ID», надалі скорочено «UID")
Ідентифікатор користувача або UID – це псевдонімний ідентифікатор користувача, такий як ідентифікатор cookie або мобільний ідентифікатор реклами (наприклад, IDFA в iOS). UID, який використовується для постійної ідентифікації браузера, комп'ютера або пристрою, відповідно до GDPR вважається "**цифровим ідентифікатором**" і є персональними даними.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180802_IABEU-GIG-Working-Paper05_Controller-Processor-Criteria.pdf

Оператор чи Контролер? – Критерії, які слід враховувати компаніям в сфері цифрової реклами

У законодавстві ЄС про приватність існують лише дві основні категорії суб'єктів, які збирають і обробляють дані: контролери даних і оператори даних. Це відрізняється від класифікацій, що широко використовуються у світі рекламних технологій США, де виділяють: Перші особи (тобто веб-сайти та рекламодавці), Треті особи (переважно технологічні компанії в сфері цифрової реклами) і Постачальники Послуг (практично агенти Першої Особи). Рекламодавці є Першими особами в багатьох контекстах (наприклад, коли вони взаємодіють безпосередньо з користувачами на своїх веб-сайтах або в разі наявності попередніх взаємовідносин), але якщо вони завантажуються в контексті іншого веб-сайту, а не свого власного веб-сайту, рекламодавці виступають як Треті особи.

Постачальники послуг у США приблизно відповідають Операторам Даних в ЄС, оскільки обидва вони є агентами Першої особи / Контролера Даних. Отже, одна з ключових відмінностей між правилами приватності рекламних технологій в США та правилами приватності ЄС полягає в тому, що дві основні категорії, визначені в правилах приватності ЄС (наприклад, хто є Оператором / Контролером), не чітко відповідають тому, як дані перетікають та взаємодіють між сторонами в моделі технологій цифрової реклами. Деякі Треті особи використовують дані Першої особи поза межами наданих інструкцій Першою особою. Це поняття виникло в рамках моделі «мережі цифрової реклами» приблизно в 1997 році, коли мережа цифрової реклами брала дані з двох абсолютно різних веб-сайтів і використовувала їх для створення цільових сегментів для вже іншого непов’язаного третього веб-сайту.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180802_IABEU-GIG-Working-Paper05_Controller-Processor-Criteria.pdf

Оператор чи Контролер? – Критерії, які слід враховувати компаніям в сфері цифрової реклами

Бізнес-моделі у сфері цифрових рекламних технологій мають свої унікальні особливості. У зв'язку з цим, на ринку виникло певне нерозуміння щодо визначення різних ролей (наприклад, визначення ролі контролерів чи операторів) у моделях технологій цифрової реклами.

Крім того, чимало рішень Європейського Суду щодо захисту даних свідчить про те, що законодавство ЄС про захист даних передбачає широкий охоплюючий підхід до розподілу відповідальності між різними ролями, якщо більше ніж одна організація безпосередньо або опосередковано займається обробкою персональних даних.

Тому компаніям у сфері цифрових рекламних технологій необхідно ɨ враховувати критерії, за якими кожна компанія зможе визначити, в якій ролі вона виступає: контролера чи оператора.

Після отримання відгуків від регуляторів з питань захисту даних у ЄС та проведення значних внутрішніх дискусій Робоча група контролерів/операторів персональних даних Групи з Впровадження GDPR розкриває пропозиції та напрацювання, що допоможуть компаніям у сфері технологій цифрової реклами визначити, чи вони виступають як контролери чи оператори даних, в залежності від обставин.

Хоча ця Робоча група не надає юридичних консультацій, вона пропонує кілька критеріїв, які можуть бути корисними для визначення того, в якій ролі виступає конкретна компанія: як контролер чи як оператор. Проте, після проведення дискусій та розгляду конкретних випадків, регулятори з питань захисту даних у ЄС все ж таки дійшли висновку, що у переважній більшості випадків компанії у сфері цифрової реклами виступають в ролі незалежного контролера кінцевого користувача.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180802_IABEU-GIG-Working-Paper05_Controller-Processor-Criteria.pdf

1. Створення та використання UID (Ідентифікатора користувача)

Чи створює Ваша компанія UID для власних цілей (виключно або навіть частково)?

Якщо так, в такому випадку ваша компанія виступає контролером цього UID. Зворотно, якщо ваша компанія створює UID виключно для цілей своїх клієнтів, то припускається, що ваша компанія виступає оператором цього UID (за умови, що ваша компанія не використовує той самий UID спільно для всіх клієнтів, оскільки такий процес обробки даних робить вашу компанію контролером таких даних, як описано у пункті 2 нижче). Компанії, які використовують рекламні ідентифікатори, наприклад ідентифікатор платформи мобільних операційних систем, які створенні третіми особами, не є "авторами" таких UID і повинні враховувати чимало критеріїв. Діяти «від імені» також означає, що оператор не може виконувати обробку для власних цілей. Як передбачено статтею 28(10) GDPR, оператор порушує норми GDPR, виходячи за рамки інструкцій контролера та починаючи визначати власні цілі та засоби обробки. Оператор вважатиметься контролером щодо такої обробки та може бути підданий санкціям за вихід за межі інструкцій та розпоряджень контролера.

На приклад, один UID може бути пов'язаний з кількома окремими наборами даних, що обробляються однією компанією (наприклад, поведінкові дані з певного веб-сайту, обробка яких проводилась від імені певного клієнта, дані про розміщення реклами з веб-сайту видавця, яких використовували для оптимізації послуг). У таких випадках відповідна компанія виступає в ролі контролера UID, які входять до різних наборів даних.

Наприклад, якщо ваша компанія створює UID, який використовується вашою компанією або спільно використовується клієнтами (виключно для цілей клієнтів), і цей UID синхронізується з UID іншого постачальника в рамках транзакції, ініційованої від імені клієнта, така синхронізація може розглядатися як технічні та організаційні заходи обробки.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180802_IABEU-GIG-Working-Paper05_Controller-Processor-Criteria.pdf

2. Сегрегація UID

Чи ізолює Ваша компанія свої UID? Іншими словами:

Чи передається або використовується UID, згаданий у пункті 1, між клієнтами вашої компанії таким чином, що один і той самий ідентифікатор користувача використовується для одного або кількох з цих клієнтів або:

Чи має кожен клієнт власний UID для кожного користувача таким чином, що один і той самий користувач може мати, наприклад, UID123 для Клієнта 1 і UID456 для Клієнта 2?

На основі наведених прикладів та критеріїв, якщо ваша компанія створює UID для власних цілей і/або передає або використовує той самий UID між клієнтами, і вам не заборонено договірним або технологічним шляхом використовувати UID для будь-яких цілей, крім виконання вказівок Контролера, передбачається, що ваша компанія є контролером цього UID. Згідно з висновками Робочої групи Статті 29, питання визначення засобів з точки зору технічних та організаційних заходів може, в певній мірі, бути делеговано операторам, за умови, що це не стосується суттєвих елементів засобів обробки даних.

На практиці, якщо надані послуги не спрямовані конкретно на обробку персональних даних або якщо така обробка не є ключовим елементом послуги, постачальник послуг може мати можливість самостійно визначати цілі та засоби такої обробки, необхідні для того, щоб надати послугу. У такій ситуації постачальника послуг слід розглядати як окремого контролера, а не як оператора. Проте аналіз кожного окремого випадку залишається необхідним, щоб з'ясувати ступінь фактичного впливу кожного суб'єкта на визначення цілей і засобів обробки. [1]

1. Керівні принципи 07/2020 щодо понять контролера та оператора в GDPR Версія 1.0, прийнято 02 вересня 2020 року Європейською радою із захисту даних.

3. Використання даних

Ваша компанія вбудовує або використовує UID (необов'язковий) чи поєднує чи іншим чином дані між клієнтами, наприклад, для оптимізації розміщення реклами, як-от обмеження частоти показів на кількох сайтах або додатках? Якщо ТАК, то вашу компанію, вважатимуть контролером таких даних.

Робоча група вирішила не проводити комплексний аналіз практик ринку рекламних технологій. Замість цього, члени групи погодилися, що компанії, які займаються оптимізацією показу реклами на кількох сайтах різних клієнтів, зазвичай вважаються контролерами цих даних. Робоча група вирішила встановити планку на рівні оптимізації показу реклами і дозволила кожній окремій компанії визначити, наскільки використання компанією даних порівнюється з оптимізацією показу реклами після консультації з відповідальною особою із захисту персональних даних.

Отже, якщо ваша компанія: 1) створює або використовує UID для власних цілей, 2) використовує той самий UID для різних клієнтів без обмежень, і 3) використовує дані, пов'язані з цим UID, для оптимізації показу реклами, такої як наприклад обмеження частоти показу на кількох сайтах, тоді ваша компанія вважатиметься незалежним контролером. Будь-який з трьох критеріїв може призвести до того, що компанія вважатиметься контролером, але концепції контролерів і операторів є функціональними і будуть залежати від конкретних обставин. Одна компанія може бути контролером щодо одного набору даних і оператором щодо іншого. У певних обставинах дані цих окремих наборів даних можуть частково співпадати. Ці критерії призначені як орієнтир щоб допомагати компаніям визначати, в якому значенні вони повинні враховувати свій статус у екосистемі цифрової реклами.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/06/20180802_IABEU-GIG-Working-Paper05_Controller-Processor-Criteria.pdf

Оцінка впливу на захист персональних даних (DPIA) для цифрової реклами відповідно до GDPR

Зміст

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

1.1 Мета цього посібника та спосіб його використання

Примітка: IAB Europe та IAB UK працювали над розробкою цього посібника спільно. Ця версія не призначена для визначення правил, які застосовуються в окремих юрисдикціях, і не передбачає, що обробка персональних даних регулюється певним регулятором. Хоча посібник надає конкретні приклади з різних юрисдикцій, він переважно базується на прямому тлумаченні вимог GDPR. Компанії, чия обробка персональних даних регулюється ICO Великобританії, можуть звернутися до аналогічної версії цього посібника, доступного в IAB UK на сайті www.iabuk.com.

Мета цього посібника – надати практичний посібник із проведення оцінки впливу на захист персональних даних (DPIA) відповідно до GDPR. У цьому документі міститься передумова та опис процесу DPIA в контексті обробки персональних даних у рекламних технологіях, для цифрової реклами загалом і для RTB, щоб допомогти компаніям зрозуміти свої обов'язки та як їх виконувати на практиці. Мета полягає в тому, щоб забезпечити прийнятний, широко прийнятий стандарт для оцінки та управління ризиками, пов'язаними з обробкою персональних даних у галузі, який може змінюватися з часом відповідно до нормативних змін і ринкової практики. Європейська рада із захисту персональних даних (EDPB) спеціально заохочує такий тип галузевої структури DPIA через те, як її можна сформувати відповідно до конкретних типів персональних даних, обробки та ризиків, які виникають у галузі.
Цей посібник має на меті конкретизувати існуючі вказівки в контексті типової цифрової рекламної діяльності та обробки персональних даних.

Цей інструкційний документ не призначений для того, щоб надати форму, яку потрібно заповнити, або надати конкретний зміст для вашого DPIA, а скоріше є путівником, який допоможе включити процес DPIA в звичайну діяльність з проектування та розробки продуктів вашої компанії. Компанії повинні адаптувати цей підхід у будь-якому форматі, який найкраще підходить до способу їх роботи. Ви можете створити його у формі енциклопедії, чи електронної таблиці, чи в інструменті відстеження проблем, або в будь-якій комбінації цих варіантів.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

1.1 Мета цього посібника та спосіб його використання

Посібник також є достатньо простим, і його можуть успішно використовувати будь-які ваші співробітники, незалежно від розміру компанії, це особливо корисно, якщо ваша компанія недостатньо велика, щоб мати армію юристів, фахівців з комплаєнсу та зовнішніх консультантів. Посібник не покладається на глибоке академічне розуміння застосовного законодавства про конфіденційність і теорії управління ризиками. Фактично, основною умовою для успішного та належного використання структури DPIA є чітке розуміння розглянутої обробки персональних даних, усіх можливих ризиків, які можуть виникнути внаслідок обробки, та ефективності доступних підходів до зменшення та врегулювання ризиків. Тому зауважте, що цей посібник не містить юридичних порад чи аналізу. Він фактично є путівником з орієнтирами для побудови правильного процесу проведення DPIA у галузі. У ньому висвітлюються ключові питання та пропонуються підходи до певних концепцій, що стосуються нашої галузі, у спосіб, який є зрозумілим для інженерів, менеджерів з продукції та іншого персоналу, який не займається конфіденційністю/юридичними питаннями.

Слід пам’ятати, що значна кількість юридичних нюансів і деталей обов’язково залишається на розсуд вашої компанії та юристів. Цей посібник не є окремим документом, і його слід читати та використовувати в контексті повного розуміння більш широких принципів і вимог GDPR, зокрема, чи потрібен і коли потрібен DPIA, а також роль Відповідальної особи з питань захисту персональних даних (DPO), і його слід читати разом з іншими відповідними посібниками. Ми позначили деякі з цих матеріалів у цьому документі, а Додаток у кінці містить детальний перелік.

1 "Європейська рада із захисту персональних даних (EDPB) заохочує розробку секторальних структур DPIA. Це пояснюється тим, що вони можуть спиратися на конкретні галузеві знання, тобто DPIA може розглядати специфіку певного типу операцій обробки (наприклад: певні типи даних, корпоративні активи, потенційні наслідки, загрози, заходи). Це означає, що DPIA може вирішити проблеми, які виникають у певному економічному секторі або під час використання певних технологій чи виконання певних типів операцій з обробки». Інструкції EDPB, с. 17. EDPB Рекомендації щодо оцінки впливу на захист даних (DPIA) і визначення того, чи може обробка «спричинити високий ризик» для цілей Регламенту 2016/679, доступні за адресою
https://ec.europa.eu/newsroom/document.cfm?doc_id=47711
2 Див. наприклад:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia

1.2 Для кого призначений цей посібник?

В першу чергу посібник призначений для використання компаніями цифрових рекламних технологій різного характеру та типу, а також рекламодавцями, агентствами та паблішерами, які співпрацюють з ними та обмінюються персональними даними або отримують персональні дані від них.

У компаніях, які використовують цей посібник, рекомендується створити міжфункціональну команду, включно з такими ролями, як менеджери з продукції, інженери, бізнес-менеджери, фахівці з конфіденційності та юристи, щоб перевести інструкції у форму та формат, які добре підходять для внутрішніх процесів компанії.

Відповідальність за процес DPIA має бути надана одному або декільком працівникам, які мають рівень знань і стаж роботи, який дозволяє їм забезпечити належне виконання процесу від початку до кінця.

Однак кожен працівник, який бере участь в обробці персональних даних, повинен розуміти свою особливу роль у цьому процесі та відповідати за неї. DPIA – це командна робота. Тому навчання відповідних працівників має бути ключовою частиною впровадження процесу DPIA.

Компанії, які мають відповідальну особу з питань захисту персональних даних (DPO), — а більшість компаній, що використовують DPIA повинні його мати — повинні проконсультуватися зі своєю DPO під час проведення DPIA та задокументувати його рекомендації як частину процесу (див. розділ 3, щоб дізнатися більше про те, хто має бути у вашій команді DPIA).

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

1.3 Сфера застосування цього посібника

Цей підхід спрямований на оцінку ризику від функцій обробки персональних даних, пов'язаних із цифровою рекламою програматик, тобто рекламними технологіями та RTB. Він не призначений для загальної обробки бізнес-даних, навіть у рекламних компаніях. Цей підхід базується на загальних даних і ризиках, пов'язаних із цифровою рекламною діяльністю. Інструкції та приклади не є повними, вичерпними чи остаточними. Компанії, які використовують ці інструкції, повинні врахувати місцеві юридичні нюанси і свої обставини, а також повинні розглянути, чи існують типи даних або ризиків, які застосовуються до їхніх обставин, але не представлені в цих матеріалах.

У цьому посібнику використовується таксономія дій із обробки – або цілей і функцій – розроблена в рамках IAB Europe Transparency & Consent Framework (TCF або Стандарти Прозорості та Згоди). Ми використовуємо TCF тому, що це надає вичерпну та корисну таксономію, а також тому, що багато, можливо, більшість компаній у цій галузі використовуватимуть TCF і, отже, узгодять свою діяльність із відповідністю визначенням TCF. Узгодивши наш посібник з TCF, наприклад, компанія може безпосередньо пов'язати свій процес DPIA з аналізом законної підстави для цілей TCF, якими вона займається. Тим не менш, кожна компанія зобов'язана гарантувати, що вона відповідає за відповідність обробки своїх власних унікальних даних. Ключовий принцип, який лежить в основі цього процесу, полягає в тому, що це не вправа для дотримання формальності, й тому її не слід виконувати механічно, а скоріше її потрібно ретельно пристосовувати до кожної окремої обставини. Це не малюнок за номерами, і один розмір не підходить усім.

Пам'ятайте також, що згідно з принципом підзвітності GDPR ви повинні мати можливість продемонструвати свою відповідність, і тому ваші записи щодо DPIA повинні бути достатньо детальними та описовими, щоб ваші міркування та прийняття рішень були чіткими та зрозумілими для інших (наприклад, наглядовим органам), якщо їм знадобиться їх переглянути.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

1.4 Зв’язок між LIA та DPIA

Ви можете помітити схожість між оцінкою законних інтересів (LIA) і DPIA. Як LIA, так і DPIA можуть бути передумовою для обробки персональних даних. Вони вимагають глибокого розгляду потенційних впливів на конфіденційність (приватність) суб'єкта даних і передбачають розгляд компромісів між цілями контролера щодо обробки та інтересами, правами та свободами суб'єкта даних.

У той час як DPIA – це процес, який використовується для виявлення та зменшення ймовірності високих ризиків для суб'єктів даних, LIA – це правовий аналіз – у ситуації, коли ви визначили законні інтереси як передбачувану законну основу для обробки персональних даних – який перед обробкою персональних даних ви зобов'язані визначити, щоб зрозуміти, чи інтереси контролера та суб'єкта даних достатньо збалансовані, щоб дозволити обробку без отримання згоди суб'єкта даних. Майже в усіх випадках компанія повинна завершити процес DPIA до завершення LIA.

І якщо передбачуваною правовою підставою для обробки є законні інтереси, під час виконання DPIA слід пам’ятати про тест на баланс LIA. Коли ви приступите до LIA, результати DPIA, зокрема залишкові ризики, будуть важливими вхідними даними для LIA. Фактично, якщо ваш DPIA було проведено ретельно і правильно, більшість основної роботи для LIA буде вже виконана. Якщо ви обробляєте персональні дані на основі законних інтересів або збираєтеся це зробити, але ще не завершили процес DPIA, вам слід подумати, чи він потрібний, особливо якщо ваша LIA показує значні ризики. Щоб отримати додаткові відомості про LIA, перегляньте наші вказівки щодо LIA.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

2.1 Що таке DPIA?

Оцінка впливу на захист персональних даних (DPIA - Data Protection Impact Assessment) - це процес управління ризиками, який має на меті об'єктивно оцінити ризики для прав осіб та вжити заходів для їх зменшення. Це не просто вправа з обґрунтування постфактум, а динамічна дія, яка передбачає постійне ведення обліку та зменшення ризиків у процесах розробки продукту. Хоча кожна організація повинна враховувати свої унікальні обставини при проведенні DPIA, застосування галузевого підходу допомагає привести процес у відповідність до галузевих стандартів і загальноприйнятих ризиків, а також включати дані, які часто використовуються.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

2.2 Коли необхідний DPIA?

Усі контролери персональних даних повинні враховувати ймовірність і серйозність ризику для фізичних осіб у своїй діяльності з обробки персональних даних, навіть якщо DPIA не є обов'язковою. Однак, відповідно до GDPR, DPIA є обов'язковою, якщо діяльність з обробки персональних даних може призвести до високого ризику для прав і свобод фізичних осіб. Конкретні випадки, що вимагають проведення DPIA, визначені в GDPR, а місцеві наглядові органи (НО) можуть також складати власні переліки операцій з обробки даних, які вимагають проведення DPIA. EDPB (Європейська рада з питань захисту персональних даних) опублікувала розширені рекомендації щодо DPIA, включаючи дев’ять критеріїв, які повинні враховуватися НО при створенні переліків. Крім того, EDPB надала висновки щодо застосування своїх критеріїв до національних переліків за допомогою механізму узгодженості, як це передбачено GDPR

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

2.2 Коли необхідний DPIA?

На практиці, перед початком будь-якої нової обробки персональних даних необхідно визначити, чи потрібно проводити DPIA, беручи до уваги GDPR та відповідні тригери. DPIA повинна бути заповнена до початку обробки і може охоплювати одну операцію або групу подібних операцій.

Організації мають можливість обґрунтувати та задокументувати, чому DPIA не потрібна для певних видів обробки. Однак застосування стандартного підходу до DPIA допомагає забезпечити дотримання вимог, включає конфіденційність за замовчуванням і підвищує обізнаність про характер обробки та пов'язані з нею ризики в компаніях.

Недотримання вимог може призвести до штрафів. DPIA є цінним інструментом незалежно від вимог і узгоджуються з принципом конфіденційності (приватності) за проєктуванням та підходами за замовчуванням при розробці продуктів.

«Операція з обробки може відповідати критеріям високого ризику EDPB, але контролер може вважати, що вона "ймовірно не призведе до високого ризику». У таких випадках контролер повинен обґрунтувати та задокументувати причини непроведення DPIA, а також включити/записати точку зору відповідальної особи з питань захисту персональних даних». Рекомендації EDPB, с. 12.

У контексті цифрової рекламної індустрії, зокрема торгів у режимі реального часу (RTB), більшість операцій з обробки персональних даних, ймовірно, спричинятимуть DPIA на основі стандартних тригерів, встановлених EDPB та національними регуляторними органами. Тому пропонується, щоб процес DPIA був галузевим підходом за замовчуванням, визнаючи, що юридичне рішення про те, чи потрібен DPIA, зрештою, залишається за кожною компанією/ організацією. Важливо зазначити, що застосування процесу DPIA не означає, що всі процеси в галузі є високоризиковими, а радше вважається найкращою практикою через наявність індикаторів ймовірного високого ризику в багатьох галузевих процесах, визначених EDPB.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3. Як створити DPIA

Як ми підкреслювали вище, DPIA – це процес, а не продукт. Це має бути ітеративний процес, який виконується в звичайному ході розробки продукту, принаймні за потреби (як зазначено вище), якщо це не відбувається за замовчуванням для всіх процесів, як ми пропонуємо.

Крім того, слід враховувати результати DPIA: обробка не повинна розпочинатися, доки не буде застосовано процес DPIA та прийнято рішення щодо продовження, і якщо на момент завершення вашої DPIA існує залишковий високий ризик, ст. 36 вимагає консультації з НО перед обробкою.10 Якщо це так, використовуйте цю інформацію, щоб ретельно обміркувати, чому існують залишкові високі ризики та чи обробка необхідна, чи може бути виправданою та чи відповідає іншим вимогам GDPR, таким як принцип справедливості.

Як зазначалося вище, незалежно від вимог DPIA, GDPR вимагає від контролерів персональних даних оцінювати ризик для суб'єктів даних у зв’язку з обробкою їхніх даних. Однак ваш процес розробки, DPIA та конфіденційність (приватність) загалом, — як вимога GDPR 13 — мають бути включені у нього, а не бути паралельним процесом. Більшість компаній не починатимуть з нуля. Вони адаптуватимуть і покращуватимуть існуючі процеси для впровадження цього керівництва DPIA. Можливо, деякі компанії значною мірою вже проводять DPIA, але їм потрібно додати формальності та документацію. Для інших включення DPIA включатиме багато суто нових процесів і, ймовірно, значні спроби та помилки, перш ніж вони зможуть добре налагодити цей процес.

10 Наприклад, дев’ять критеріїв EDPB включають: оцінку, включаючи «поведінкові або маркетингові профілі», систематичний моніторинг, конфіденційні або чутливі персональні дані, дані, оброблені у великому масштабі, зіставлення або об’єднання наборів даних та інноваційне використання технологій. Національні списки НО постійно включають тригери, які включають різні функції в індустрії цифрової реклами, такі як відстеження, невидима обробка, аналітика великої кількості даних, профілювання для маркетингу, збір історії веб-переглядів, дані, зібрані через Треті сторони, спостереження за поведінкою суб’єктів даних в Інтернеті тощо.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.1 Загальні зауваження

i. Примітка щодо об’єктивності та необхідності.
У цьому документі йдеться про об’єктивний аналіз або точку зору суб'єкта даних, а також про необхідність обробки. Об’єктивність означає відступ і погляд ззовні вашої компанії. Необхідність передбачає питання про те, чи можна використовувати альтернативу, яка менш порушує конфіденційність (приватність). Цей аналіз - справжнє мистецтво, оскільки все залежить від вашої точки зору та рівня абстракції.
Повне обговорення об’єктивності, збалансованості, 12
Коли наглядовий орган проводить консультації, він оцінює DPIA. Наприклад, у своїх інструкціях ICO Великобританії зазначає: "Ми надамо вам письмову відповідь, у якій буде повідомлено, чи є ризики прийнятними, або чи потрібно вам вжити подальших дій. У деяких випадках ми можемо порадити вам не виконувати обробку, оскільки ми вважаємо, що це буде порушенням GDPR. У відповідних випадках ми можемо видати офіційне попередження або вжити заходів, щоб повністю заборонити обробку даних."
Див. protection-regulation-gdpr/accountability-and-governance/dataprotection-impact-assessments/#dpia5 13 GDPR ст. 25 встановлює вимоги щодо захисту персональних даних за проєктуванням і за замовчуванням, і принципи GDPR виходять за рамки цього посібника, але ваша відповідальна особа з питань захисту персональних даних та спеціалісти з питань конфіденційност (приватності)і /юристи повинні мати змогу допомогти вам.

ii. Коли починати створювати DPIA
DPIA слід починати створювати на ранніх стадіях процесу розробки продукту. Рекомендується включати міркування щодо конфіденційності (приватності) на стадіях концепції та ідеї, щоб гарантувати, що розробка відображатиме конфіденційність (приватність) за проєктуванням і за замовчуванням, що є вимогою GDPR. Якщо оцінка конфіденційності (приватності) та DPIA виконуються надто пізно в процесі, то ви втрачаєте час та упускаєте можливості для кращої конфіденційності (приватності), змушуючи свою компанію йти на неоптимальні компроміси та ризикувати невідповідністю (наприклад, статті 24, 25, 32, 35, 36, які охоплюють обов’язки контролера даних; захист персональних даних за проєктуванням і за замовчуванням; безпеку; вимоги DPIA).

3.1 Загальні зауваження

iii. Хто бере участь у DPIA.

DPIA має проводитися міжфункціонально групою експертів, які індивідуально та колективно представляють знання, експертизу та досвід, необхідні для глибокого розуміння контексту обробки та ризиків для прав суб'єктів даних. Наприклад, команда DPIA може складатися зі звичайної команди продукту – менеджерів продукту, інженерів, дизайнерів, персоналу з інформаційної безпеки – доповненої фахівцем з конфіденційності та періодично включати відповідальну особу з питань захисту персональних даних для консультацій, зокрема в кінцевій точці, коли ви приймете остаточне рішення щодо того, продовжувати обробку чи ні.

iv. Використання методичних матеріалів

Ці керівні матеріали не призначені для використання в готовому вигляді, тут не існує універсального підходу. Візьміть наведені тут матеріали як основу та включіть їх у свій власний індивідуальний процес, який відповідатиме способам роботи вашої компанії та сценаріям, які ви оцінюєте. Використовуйте будь-які інструменти, які забажаєте: електронні таблиці, засоби відстеження помилок, системи контролю версій, енциклопедію.

Незалежно від того, що ви використовуєте, воно має містити записи про ваш процес і рішення, які ви приймаєте під час роботи, і записи слід постійно оновлювати. Зрештою, ви повинні мати можливість вказати на записи, які демонструють обґрунтованість вашого процесу DPIA, а ваша документація має бути достатньо детальною та описовою для особи, яка не є експертом у вашій галузі (наприклад, регулятора), щоб вона могла все зрозуміти.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.2 Огляд процесу та етапів

DPIA та конфіденційність (приватність) за проєктуванням вимагають процесу ітерації (й іноді узгодження). Як показано на діаграмі нижче, в основі процесу лежить ітераційний цикл, за допомогою якого оцінюється використання персональних даних, усвідомлюються ризики, застосовуються заходи пом'якшення ризиків. Цикл повторюється за потреби, поки не буде досягнуто певної міри остаточного стану, після чого приймається рішення про те, чи вплив обробки на суб'єктів даних (індивідуально чи колективно) є прийнятним і чи має продовжитись обробка, а «кінцевий» продукт може бути оцінений на повну відповідність вимогам GDPR.

Звичайно, якщо після проходження процесу DPIA після обробки залишається високий ризик, ви повинні проконсультуватися з наглядовим органом, як того вимагає ст. 36 (як описано в розділі 3.3). Ви повинні підходити до процесу об'єктивно та відкрито, використовуючи його як інструмент для прийняття рішень і бути готовими до різних результатів, зокрема до того, що ви можете виявити ризики, які неможливо належним чином пом'якшити, і це означає, що обробка, яку ви оцінюєте, не може бути виконана.

Примітка: наведений тут цикл є ілюстративним, заснованим на типових циклах розробки продукту, але не є обов'язковим. Він показує кроки, які ви повинні пройти, але точний порядок і послідовність можна адаптувати відповідно до ваших конкретних обставин.

Насправді це не робиться такими окресленими етапами, але скоріше відображає якість виконання, або принаймні кроки, які потрібно мати на увазі, всі етапи одночасно в процесі розробки продукту. З самого раннього етапу розробки продукту, ви повинні подумати про свій шлях до забезпечення того, щоб обробка персональних даних була необхідною, справедливою, виправданою і, звичайно, законною.

Огляд етапів*

Створіть команду DPIA.
Коли починається розробка продукту? При першому задумі чи ідентифікації потреби? Чи під час виникнення ідеї? У фазі дослідження та експериментування? Кожна компанія матиме власний процес, але процес DPIA має розпочатися раніше. Питання конфіденційності (приватності) слід брати до уваги з самого раннього етапу, відображаючи захист персональних даних за проєктуванням і за замовчуванням, що означає залучення потрібних людей на ранній стадії та визначення потрібних людей, відповідальних за контроль і затвердження проекту наприкінці.

Встановіть цілі обробки.
Чітко, об'єктивно, поясніть, чого саме має досягти обробка персональних даних і як обробка призводить до очікуваного результату. Це важливо для більшості етапів процесу: зменшення ризиків, законність, пропорційність. Розумно та прийнятно групувати споріднені або подібні дії обробки, тому ви можете мати кілька цілей.

Встановіть контекст обробки
Контекст включає всі важливі факти про обробку: персональні дані, які будуть використані, потік через різні системи, час, протягом якого персональні дані потрібно зберігати, місце зберігання, транскордонні передачі, передачі третім особам тощо. Контекст може бути конкретизованим і може розвиватися з часом, коли команда повторюватиме процес.

Переконайтеся, що всі члени команди повністю розуміють цілі та контекст.
Вкрай важливо переконатися, що всі члени команди добре розуміють цілі та контекст і погоджуються з ними. Без повного розуміння цілей і контексту член команди не може повноцінно брати участь у процесі. Він або вона не в повній мірі готові визначити ризики та запропонувати, як їм запобігти, щоб забезпечити відповідність цілям. Подібним чином, без узгодження між командою процес не працюватиме належним чином. Оскільки процес розробки продукту рухається швидко, часто люди замовчують деталі чи розбіжності та роблять припущення, не ставлячи питань. Часто значна кількість часу витрачається на безплідні розмови, тому що залучені люди не мають спільного розуміння цілей та/або контексту. Ось чому це включено тут як чіткий крок.

Огляд етапів*

Застосуйте методи мінімізації персональних даних і конфіденційності (приватності) за проєктуванням (PBD).

Кожна компанія повинна застосовувати цей підхід у процесі розробки продукту. Цього вимагає GDPR. Це означає вибір проєктування на користь конфіденційності (приватності) – впровадження принципів захисту персональних даних і захисту прав і свобод суб'єктів даних – на ранніх стадіях процесу розробки, і це означає скорочення обробки персональних даних до мінімуму, необхідного для досягнення ваших цілей, або можна навіть розглянути альтернативи, які сприяють більшій конфіденційності (приватності). Нижче наведено подальше обговорення загальних методів.

Оцініть ризики.
Враховуючи контекст – персональні дані, що підлягають обробці, збереженню, обміну тощо – і після застосування методів мінімізації даних і PBD, які можливі ризики існують для прав і свобод суб'єкта даних? Нижче наведено подальше обговорення того, як визначити й оцінити ризики, а також обговорення загальних ризиків, пов’язаних з обробкою в індустрії цифрової реклами.

Застосуйте заходи щодо запобігання або зниження ризиків
Це окремий крок що відрізняється від мінімізації персональних даних і конфіденційності (приватності) за проєктуванням (обидва кроки є окремими вимогами), навіть якщо вони всі є заходами щодо запобігання або зниження ризиків конфіденційності (приватності). Метою цього кроку є застосування додаткових засобів з урахуванням ризиків, які залишаються після мінімізації та забезпечення конфіденційності (приватності) на етапах проектування.

Повторюйте, доки не закінчите.
У якийсь момент цикл завершується. Ризики визначено та оцінено, застосовано заходи щодо запобігання або зниження ризиків, і нічого більше не зробиш. На цьому етапі у вас є «остаточний» дизайн (проєкт) продукту, якому можна дати остаточну оцінку на наступному етапі щодо того, чи готовий він до виробництва.

Огляд етапів*

Визначте залишкові ризики та оцініть їх відповідно до принципів GDPR, таких як справедливість і пропорційність.
На відповідній стадії процесу розробки, ви можете подивитися на те, що у вас є, і оцінити, чи відповідає обробка персональних даних потребам і ризикам, і чи відповідаєте ви правовим вимогам для досягнення законних підстав, згідно з якими ви будете проводити обробку, а також чи відповідає обробка принципам і вимогам GDPR. Це має бути об'єктивний аналіз, і якщо обробка, запропонована в цьому «кінцевому» стані, все ще створює високий ризик, ви повинні повернутися назад і знайти альтернативи; вирішити не продовжувати далі; або проконсультуватись зі своїм наглядовим органом, як того вимагає ст. 36. Ви маєте залучити до цього аналізу свою відповідальну особу з питань захисту персональних даних та, можливо, вище керівництво (і/або будь-кого, кого ви визначили як такого, хто має право на остаточне схвалення продукту).

Підтримка DPIA, включаючи дотримання заходів щодо запобігання або зниження ризиків
DPIA створює постійне зобов'язання. Ви повинні переконатися, що ваш аналіз залишається вірним. Досягти цього можна оновлюючи контекст обробки та проводячи повторну оцінку, коли відбуваються зміни. Таким чином ви гарантуєте, що ваша компанія дотримується правил конфіденційності (приватності)за замовчуванням, мінімізації персональних даних і зниження ризиків.

Зауважимо, що є фактичний та аналітичний етапи процесу. Не зволікайте ні з одним, ні з іншим. Для аналізу необхідна міцна основа з фактичної інформації

3.3 Процес DPIA.
Етап 1: Створіть команду

Коли починається розробка продукту? При першому задумі чи ідентифікації потреби? Чи під час виникнення ідеї? У фазі дослідження та експериментування? Кожна компанія матиме власний процес, але процес DPIA має розпочатися раніше.

Питання конфіденційності (приватності) слід брати до уваги з самого раннього етапу, відображаючи захист даних за проєктуванням і за замовчуванням, що означає залучення потрібних людей на ранній стадії та визначення потрібних людей, відповідальних за контроль і затвердження проєкту наприкінці.

Визначте, хто бере участь у процесі DPIA.
- Менеджери продуктів та інженери, що розробляють продукт(и)
- Менеджери/інженери з питань конфіденційності
- Співробітники інформаційної безпеки
- Дизайнери UI/UX
- Спеціаліст/юрист з питань конфіденційності
- DPO (відповідальна особа з питань захисту персональних даних)

Визначте, хто несе остаточну відповідальність за завершення DPIA?
Визначте, хто, крім DPO, повинен підписувати DPIA, зокрема, щодо залишкового ризику?

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.3 Процес DPIA.
Етап 2: Встановіть цілі обробки

Чітко, об’єктивно, поясніть, чого саме має досягти обробка персональних даних і як обробка призводить до очікуваного результату. Це важливо для більшості етапів процесу: запобігання і зменшення ризиків, законності, пропорційності. Прийнятно групувати споріднені або подібні дії обробки персональних даних, тому ви можете мати кілька цілей.

Узагальнено опишіть, який продукт чи продукти розробляються, характер обробки персональних даних, а також цілі продуктів/обробки. Включіть до уваги наступне:

- Чого ви сподіваєтеся або маєте намір досягти?
- Які будуть переваги для вашої компанії, суспільства, суб'єкта даних?

Це можна зробити прозою або у формі презентації, діаграми або у будь-якій іншій формі, яка вам найкраще підходить, за умови, що ви будете дуже ретельними, і матеріали будуть забезпечувати достатню основу для всього залученого персоналу. Суть полягає в тому, щоб мати записи та довідкові матеріали, доступні для команди, яка працюватиме над продуктом.

Ви повинні мати можливість узгодити обробку з цілями та показати необхідність усієї обробки для конкретних цілей. Потрібно подумати про цілі та необхідність обробки з різних точок зору. Хоча певна обробка може знадобитися для того, щоб певний продукт працював, це не обов’язково означає, що ви можете або повинні шукати виправдання на цій основі.

Можливо, існує альтернативний продукт або проєкт (дизайн), які б відповідали вашим цілям з меншим втручанням або ризиком для конфіденційності людей.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.3 Процес DPIA.

Етап 3: Встановлення контексту обробки

Контекст включає всі відповідні факти про обробку: персональні дані, які будуть використані, потік через різні системи, час, протягом якого потрібно зберігати дані, місце їх зберігання, транскордонні передачі, передачі третім особам тощо. Контекст може бути конкретизованим і може розвиватися з часом, коли команда повторюватиме процес.

Ви повинні детально визначити всі фактичні обставини обробки. Цей контекст буде оновлюватися з часом і з розвитком дизайну продукту. Ви повинні пояснити, чому обробка цих даних необхідна для досягнення ваших цілей.

Нижче наведено деякі речі, які слід враховувати під час цього процесу. Цей список не є вичерпним. Добре подумайте про свої конкретні обставини. Крім того, вам слід планувати взяти до уваги більш детальні вказівки щодо цих питань від IAB, регуляторів та з інших джерел.

- Які типи персональних даних обробляються? (Зверніться до Додатку A, щоб отримати неповний список типів даних, які зазвичай використовуються, а також деякі примітки щодо кожного.)
- Які методи ідентифікації та підтримки ви будете використовувати?
- Чи будете ви обробляти конфіденційні дані або дані спеціальної категорії? (Чи можливо таке, що ви будете це зробити, навіть якщо не збирались, наприклад, через запити ставок або виклики пікселів?)
- Чи будете ви зберігати та/або отримувати доступ до інформації на пристрої (ціль 1 TCF)? Якщо так, то як ви отримаєте згоду?
- З яких географічних районів збиратимуться дані?
- Приблизно від скількох суб'єктів даних будуть оброблені дані (у порядку величини, тобто тисячі, сотні тисяч, мільйони)?
- Які у вас стосунки з суб’єктами даних?
- Де зберігатимуться персональні дані?
- Чи задіяні будь-які оператори персональних даних? Якщо так, вам потрібно детальніше розповісти, як ви керуєте ризиками, пов’язаними з використанням операторів.
- Чи будуть переміщення або зберігання персональних даних поза національними кордонами? Якщо так, то де?
- Який ваш графік деідентифікації, анонімізації та/або видалення персональних даних для всіх персональних даних? (Див. примітки щодо цієї теми в розділах мінімізації та запобігання ризикам.)
- Чи будете ви поєднувати дані з різних джерел або контекстів? Якщо так, опишіть усі джерела та процес зіставлення та об’єднання даних. Майте на увазі, що об’єднання даних може, залежно від низки факторів (характер даних, для чого вони використовуватимуться тощо), потенційно збільшити ризик виникнення даних спеціальної категорії.

3.3 Процес DPIA.
Етап 3: Встановлення контексту обробки

Чи включатиме обробка створення профілів?

- Детально опишіть цілі обробки. Класифікуйте цілі відповідно до таксономії TCF, наскільки це можливо. (Зверніться до Додатку A політики TCF, щоб отримати визначення та вказівки щодо змісту кожної цілі) Окремо опишіть цілі, які не вписуються в визначення TCF. Примітка: ці цілі TCF є корисною структурою для опису контексту обробки та для узгодження обробки із законними підставами (якщо ви використовуєте TCF), але не повинні розглядатися як короткий шлях до повного опису обробки та її мети.
    - Створіть профіль персоналізованої реклами (TCF мета 3)
    - Виберіть персоналізовану рекламу (TCF мета 4)
    - Створіть профілью персоналізованого контенту (TCF мета 5)
    - Виберіть персоналізований контент (TCF мета 6)
    - Вимірюйте ефективність реклами (TCF мета 7)
    - Вимірюйте ефективність контенту (TCF мета 8)
    - Застосовуйте дослідження ринку, щоб отримати інформацію про аудиторію (TCF мета 9)
    - Розробляйте та вдосконалюйте продукти (TCF мета 10)
    - Забезпечуйте безпеку, запобігайте шахрайству та здійснюйте дебагінг (TCF спеціальне призначення 1)
    - Технічно доставляйте рекламу чи контент (TCF спеціальне призначення 2)
    - Зіставляйти та комбінуйте офлайн-джерела даних (функція TCF 1)
    - Пов’язуйте різні пристрої (функція TCF 2)
    - Отримуйте та використовуйте автоматично надіслані характеристики пристрою для ідентифікації (функція TCF 3)
    - Використовуйте точні дані геолокації (спеціальна функція TCF 1)
    - Активно скануйте характеристики пристрою для ідентифікації (спеціальна функція TCF 2)
- Інші цілі, які виходять за межі вищезазначених?
- Де і як суб'єкт даних отримує повідомлення про обробку?
- Якою мірою або якими способами обробка є новою? Це усталена модель чи нове використання персональних даних?
- Які можливості вибору має суб'єкт даних щодо обробки?
- Якщо будь-які персональні дані будуть передані третім сторонам:
    - Які причини для спільного використання?
    - Які конкретні персональні дані будуть передані?
    - Якщо одержувачі беруть участь у TCF, чи будете ви фільтрувати персональні дані на основі рядка згоди TCF (TCF Consent String)?
    - Які засоби контролю існують щодо цього обміну та будь-якої подальшої обробки, і як ці засоби контролю будуть виконуватись?

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.3 Процес DPIA.

Етап 4: Переконайтеся, що всі члени команди повністю розуміють цілі та контекст

Вкрай важливо переконатися, що всі члени команди добре розуміють цілі та контекст і погоджуються з ними. Без повного розуміння цілей і контексту член команди не може повноцінно брати участь у процесі. Він або вона не в повній мірі готові визначити ризики та запропонувати, як їм запобігти, щоб забезпечити відповідність цілям. Подібним чином, без узгодження між командою процес не працюватиме належним чином.

Оскільки процес розробки продукту рухається швидко, часто люди замовчують деталі чи розбіжності та роблять припущення, не ставлячи питань. Часто значна кількість часу витрачається на безплідні розмови, тому що залучені люди не мають спільного розуміння цілей та/або контексту. Ось чому це включено тут як чіткий крок.

Чи всі члени команди DPIA переглянули цілі та контекст обробки? Чи погоджено, що цілі та контекст обробки є точними та повними? Чи є якісь відкриті питання, непорозуміння чи розбіжності, які необхідно вирішити перед переходом до наступного етапу?

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.3 Процес DPIA.

Етап 5: Застосування методів конфіденційності (приватності) за проєктуванням і мінімізації даних

Кожна компанія повинна застосовувати цей підхід у процесі розробки продукту. Цього вимагає GDPR. Це означає вибір проєкту (дизайну) на користь конфіденційності (приватності) – впровадження принципів захисту даних і захисту прав і свобод суб'єктів даних – на ранніх стадіях процесу розробки, і це означає скорочення обробки персональних даних до мінімуму, необхідного для досягнення ваших цілей. Можливо потрібно буде навіть розглянути більш сприятливі для конфіденційності (приватності) альтернативи. Нижче наведено подальше обговорення загальних методів.

Багато написано про те, як впровадити конфіденційність (приватність) у проєкт (дизайн) продукту. Ми не розглядатимемо це тут, але наведемо деякі ресурси в розділі ресурсів (див. Додаток) нижче. Суть полягає в тому, що ви повинні – зобов’язані – враховувати конфіденційність (приватність) як невід’ємну частину проєкту (дизайну) продукту, де це можливо, а не розглядати конфіденційність (приватність) вже після створення продукту.

Однак більшість (якщо не всі) компаній у цьому секторі займаються діяльністю, яку національні НО EDPB відмітили як таку, що ймовірно має високий рівень ризику (див. розділ 3 цього посібника), тому відповідність GDPR, ймовірно, вимагатиме ретроспективного перегляду та адаптації наявних продуктів. Звичайно, для компаній-учасниць TCF може бути значною допомогою, оскільки там надаються засоби прозорості та вибору, які були недоступні до GDPR.

Таким чином, робота на цьому етапі полягає в тому, щоб застосувати методи мінімізації персональних даних і конфіденційності (приватності) при проєктуванні до процесу розробки вашого продукту або, для існуючих продуктів, переглянути їх через цю призму.

У рамках цього ви завжди повинні думати про те, чи шлях розробки продукту, який ви обрали, є правильним, і чи можуть бути доступні інші альтернативи, які менше порушують конфіденційність (приватність) .

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.3 Процес DPIA.

Етап 5: Застосування методів конфіденційності (приватності) за проєктуванням і мінімізації даних

Отже, для кожної мети обробки та типу персональних даних, описаних у контексті обробки, подумайте про наступне:

- Чи можете ви досягти своїх цілей, обробляючи меншу кількість персональних даних або взагалі не обробляючи їх?
- Де ви можете використовувати обробку, яка менш заважає конфіденційності (приватності), для досягнення ваших цілей?
- Чи можете ви зробити обробку більш прозорою для суб'єкта даних?
- Де можна знизити точність даних?
- Чи зменшили ви зберігання персональних даних до необхідного мінімуму? Ви повинні мати окремий період зберігання для всіх персональних даних.
- Зверніться до Додатку А для міркувань щодо конкретних типів персональних даних. Майте на увазі, що ви повинні дотримуватися принципів GDPR, а також його практичних вимог, і ці принципи є корисним посібником для цього етапу процесу DPIA.

Інші міркування:

- Де і як суб'єкт даних отримує повідомлення про обробку? Чи можете ви запропонувати більше прозорості?
- Які можливості вибору має суб'єкт даних щодо обробки? Чи можете ви запропонувати більше вибору?
- Чи правильно ви реалізували TCF і чи застосовуєте ви сигнали TCF до цієї обробки?
- Звідки надходять персональних дані і куди вони йдуть? Чи надійне джерело (законне тощо)? Чи є у вас відповідні засоби контролю під час передачі?
- Чи достатньо описує обробку ваша політика конфіденційності (приватності)?
- Чи буде обробка точно відображена у ваших записах обробки (ROPA), як того вимагає ст. 30?

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.3 Процес DPIA.
Етап 6: Оцініть ризики

Враховуючи контекст – персональні дані, що підлягають обробці, збереженню, обміну тощо – і після застосування методів мінімізації даних і PBD, оцініть всі можливі ризики для прав і свобод суб'єкта даних. Нижче наведено подальше обговорення того, як визначити й оцінити ризики, а також обговорення загальних ризиків, пов'язаних з обробкою в індустрії цифрової реклами.

Вам потрібно розглянути, враховуючи кожну з запланованих операцій обробки персональних даних та всі залучені персональні дані, як вказано в контексті обробки, а також підходи до мінімізації персональних даних і конфіденційності (приватності), застосовані на Етапі 5, які залишаються ризики. Для кожного ризику вам необхідно об’єктивно вивчити потенційний вплив і серйозність впливу на суб'єкта даних і ймовірність його виникнення. Існує багато способів проведення оцінки ризику, і приклади методології наведено в Додатку A: Оцінка ризику.

Перегляньте таблицю загальних ризиків у цифровій рекламі в Додатку C (зауважте, що це не вичерпний список, і вам потрібно подумати про власні продукти та процеси та супутні ризики, пов'язані з ними). Що з цього стосується кожного типу персональних даних і кожної операції обробки?

Які ще ризики ви бачите? Які інші ризики стосуються ваших обставин? Думайте ширше. Перелічіть усі ризики, щоб команда могла їх розглянути. Подумайте з точки зору суб'єктів даних, які мають різний рівень здатності зрозуміти обробку персональних даних, і наслідки обробки, а також різні суб'єктивні погляди на існуючі ризики. Деякі НО висловлюють занепокоєння тим, що "…у RTB наданій інформації про конфіденційність (приватність) часто бракує ясності та вона не дає людям належного уявлення про те, що відбувається з їхніми даними".

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.3 Процес DPIA.

Етап 7: Застосуйте заходи щодо запобігання або зниження ризиків

Це окремий крок, що відрізняється від мінімізації персональних даних і конфіденційності (приватності) за проєктуванням (обидва кроки є окремими вимогами), навіть якщо вони всі є заходами щодо запобігання або зниження ризиків конфіденційності (приватності). Метою цього кроку є застосування додаткових засобів з урахуванням ризиків, які залишаються після мінімізації та забезпечення конфіденційності (приватності) на етапах проєктування.

Як пояснювалося раніше, ваша DPIA має бути ітеративним процесом, що виконується в ході звичайної розробки продукту, який допомагає вам зрозуміти, оцінити та пом'якшити вплив на конфіденційність (приватність) і зменшити ризики для суб'єктів даних. На цьому етапі ви повинні розглянути кожен із невирішених ризиків, виявлених на попередньому етапі, і спробувати застосувати подальші заходи для їх пом’якшення, щоб зменшити ці ризики або їх вплив на конфіденційність (приватність) .
Загальні заходи щодо запобігання або зниження ризиків, які використовуються в галузі, включають:

- Додаткова прозорість і контроль для суб'єктів даних
- Внутрішня політика щодо обмеження цілей, зберігання персональних даних, безпеки
- Договірні обмеження (для випадків спільного використання)
- Подальша мінімізація персональних даних

Вам також слід ознайомитися з міркуваннями щодо певних типів даних у Додатку B та примітками, пов’язаними з загальними ризиками в Додатку C, щоб краще зрозуміти ризики в нашій галузі.

Сповіщення та прозорість:

- Як ви будете повідомляти суб'єкта даних про обробку персональних даних?
- Чи в повідомленні докладно описується обробка персональних даних в простих для розуміння термінах? Наприклад, британський ICO опублікував інструкції щодо повідомлень про конфіденційність (приватність), у тому числі щодо розробки контенту та способів надання інформації про конфіденційність (приватність).
- Якщо використовується TCF, чи відповідає ваша обробка цілям і функціям, визначеним у TCF? Якщо ні, як ви з цим впораєтесь?
- Чи є обробка прозорою для користувачів? Наприклад, файли cookie є видимими для користувача, а ймовірнісні ідентифікатори – ні.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.3 Процес DPIA.

Етап 7: Застосуйте заходи щодо запобігання або зниження ризиків

Політика:

- Яка політика безпеки застосовується до даних?
- Чи контролюється доступ до персональних даних за моделлю "найменших привілеїв"?
- Яка внутрішня політика регулює використання та обмін персональних даними? Наприклад, відповідно до обробки:
    - Чи є у вас політики, що забороняють певні типи сегментів?
    - Політика заборони реклами для вразливих верств населення?
- Які засоби контролю існують для забезпечення відповідності політикам? Це важливо для забезпечення того, щоб ваша політика зменшувала ризик на практиці.

Зберігання та утримання персональних даних:

- Чи знаєте ви, де будуть зберігатися персональних дані?
- Якщо персональних дані будуть зберігатися або передаватися закордон, чи є у вас відповідні гарантії, включно з необхідними умовами договору?
- Чи є у вас окремий період зберігання для всіх персональних даних?
- Як ви гарантуєте видалення персональних даних?

Права суб'єкта даних:

- Як ви дотримуєтеся всіх прав суб'єктів даних, як того вимагає GDPR?
- Як ви реалізували право суб’єкта заперечувати проти обробки, а також не давати та/або відкликати згоду?
- Які обмеження є у вашої реалізації? Чи можете ви їх компенсувати?

Обмін даними з іншими сторонами:

- Як ви впевнитесь у виконанні політик отримувачами персональних даних перед наданням їм доступу?
- Чи укладені у вас договори з усіма отримувачами персональних даних?
- Чи є або будуть існувати договірні обмеження щодо обробки персональних даних отримувачами? Якщо так, то які вони?
- Яким чином ви звели до мінімуму персональні дані, які будуть передані?
- Як суб'єкти даних інформуються про отримання персональних даних новими контролерами?
- Як ви контролюватимете та забезпечуватимете дотримання договірних обмежень?
- Для одержувачів, які беруть участь у TCF, чи фільтруєте ви персональних дані на основі рядка згоди TCF?
- Які заходи ви вживаєте щодо отримувачів, які не беруть участі в TCF, щоб переконатися, що вони мають правові підстави для обробки даних?

Робота з операторами:

- Як ви перевіряєте операторів, щоб переконатися в їх достовірності та надійності, перш ніж надавати їм персональні дані?
- Чи є у вас DPA для всіх операторів?
- Яким чином ви мінімізували персональні дані, які передаються операторам?
- Які заходи ви будете використовувати для контролю дотримання DPA?

3.3 Процес DPIA

Етап 8: Це все?

У якийсь момент цикл завершується. Ризики визначено та оцінено, застосовано заходи щодо запобігання або зниження ризиків, і нічого більше не зробиш. На цьому етапі у вас є «остаточний» проєкт (дизайн) продукту, якому можна дати остаточну оцінку на наступному етапі щодо того, чи готовий він до виробництва.

Чи вважаєте ви, що достатньо добре завершили попередні етапи? Якщо високий ризик залишається, можливо, вам доведеться піти на компроміс зі своїми цілями, щоб застосувати більш агресивні засоби пом'якшення ризиків. Вам слід пам'ятати, що ваш продукт має відповідати принципам GDPR і законодавчим вимогам.

Якщо ви не готові, оновіть контекст обробки та повторіть цикл знову. DPIA має бути циклічним повторюваним процесом, вбудованим у розробку вашого продукту, методичного аналізу ризиків і зменшення впливу на конфіденційність (приватність). Вам слід переглянути та оновити інформацію та рішення, які ви прийняли на кожному етапі попередньої ітерації, щоб відобразити будь-які зміни (наприклад, у цілях, проєкті (дизайні) продукту тощо).

Якщо ви готові, переходьте до Етапу 9.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.3 Процес DPIA

Етап 9. Визначте залишкові ризики та оцініть їх

На відповідній стадії процесу розробки, ви можете подивитися на те, що у вас є, і оцінити, чи відповідає обробка потребам і ризикам, і чи відповідаєте ви правовим вимогам для досягнення законних підстав, згідно з якими ви будете проводити обробку, а також чи відповідає обробка принципам і вимогам GDPR. Це має бути об'єктивний аналіз, і якщо обробка, запропонована в цьому «кінцевому» стані, все ще створює високий ризик, ви повинні повернутися назад і знайти альтернативи; вирішити не продовжувати далі; або проконсультуватись зі своїм наглядовим органом, як того вимагає ст. 36. Ви залучите до цього аналізу свою DPO та, можливо, вище керівництво (і/або будь-кого, кого ви визначили як такого, хто має право на остаточне схвалення продукту).

Першим кроком на цьому етапі є визначення залишкового ризику після застосування мінімізації персональних даних і конфіденційності (приватності) за проєктуванням на етапі 5 і зниження ризиків на етапі 7. Це означає об'єктивне визначення ризиків або впливу на конфіденційність (приватність), які залишаються для прав і свобод суб'єктів даних після всіх застосованих вами заходів. Наприклад, у вказівках ICO сказано: "DPIA не обов'язково вказує на те, що всі ризики усунено. Але вона має допомогти вам задокументувати їх і оцінити, чи залишилися ризики чи ні, і наскільки вони виправдані". Необхідно розуміти залишковий ризик тому, що результати вашого DPIA повинні бути розглянуті та підписані вашою DPO (і, можливо, іншими вищими керівниками вашої організації, залежно від ваших механізмів процесу/керування), так і через те, що залишковий ризик є необхідною частиною вашого аналізу пропорційності та правової основи. Ви, за участю DPO, юристів та вищого керівництва, повинні будете оцінити, чи, враховуючи залишковий ризик або вплив на конфіденційність, обробка може бути виправданою: чи вона пропорційна, чесна, законна тощо, і чи все це відповідає вимогам GDPR? Перегляньте кожен тип персональних даних і кожну операцію обробки. Беручи до уваги мінімізацію персональних даних, PBD та зниження ризиків, які ризики залишаються? Приклади типів персональних даних і поширених ризиків див. у Додатку B і Додатку C.

Деякі приклади залишкових ризиків включають:

- Навіть з урахуванням договірних обмежень і процедур відповідності (таких як постійний моніторинг, аудити, належна обачність тощо), одержувачі персональних даних можуть використовувати персональних дані не за призначенням або дані можуть бути скомпрометовані (несанкціонований доступ до персональних даних).
- Навіть за короткого періоду зберігання та належного контролю безпеки персональні дані можуть бути скомпрометовані (несанкціонований доступ до персональних даних) або стати предметом неправильного використання внутрішніми співробітниками.
- Навіть після сповіщення суб'єкти даних можуть не повністю розуміти наслідки деяких типів обробки. Оцініть усі такі залишкові ризики та візьміть їх до уваги під час аналізу законності та пропорційності. Зверніться до Додатку B для вказівок.

3.3 Процес DPIA

Етап 9. Визначте залишкові ризики та оцініть їх

Законність

Звичайно, вам потрібно забезпечити законну підставу та загальну законність обробки. Це хороша можливість оцінити, чи, враховуючи ваш продукт, ви в змLIA відповідати вимогам обраної вами законної підстави та як ви відповідаєте іншим формальним вимогам GDPR.
Для кожної операції обробки, згода на яку буде вашою законною підставою:

- Де ви отримуєте згоду?
- Чи відповідає згода юридичним вимогам, чи була вона добровільно надана, чи вона конкретна, поінформована і недвозначна з боку суб'єкта даних?
- Якщо ви отримуєте доступ або зберігаєте персональних дані на пристрої, напр. читання/налаштування файлів cookie, як ви забезпечите згоду перед доступом до пристрою?
- Як ви зберігаєте згоду користувача?
- Як суб'єкт даних може відкликати свою згоду?
- Чи так само легко відкликати згоду, як її надати?
- Чи будете ви періодично поновлювати згоду?

Для кожної операції обробки, для якої законний інтерес буде вашою правовою основою:

- Чи завершили ви оцінку законного інтересу (LIA) за допомогою прийнятої системи або шаблону, і чи це оцінювання завершене обґрунтованим висновком про те, що переслідувані інтереси не переважають права та свободи суб'єкта даних? Ви повинні провести LIA перед тим, як розпочати обробку на цій підставі.*
- Як суб'єкт даних може заперечити проти обробки?

Як і TCF, цей шаблон передбачає, що з шести можливих законних підстав у GDPR лише згода** є дієвою правовою базою на практиці для обробки у цифровій рекламі.

Примітка: участь у TCF не є заміною для окремих учасників, які беруть на себе відповідальність за свої зобов'язання за законом. Крім того, деякі аспекти згоди навмисно не охоплюються у TCF, тому що застосовуються різні тлумачення на національному рівні.

Як ви будете виконувати право суб’єктів на видалення персональних даних?
Як ви будете дотримуватися права суб'єктів даних на доступ до персональних даних?
Чи маєте ви угоди про обробку персональних даних з усіма залученими операторами, як того вимагає ст. 28?

**До 2023 року IAB мав окремий посібник із проведення LIA для цифрової рекламної діяльності. У 2023 законні інтереси були виключені як юридична підстава для обробки персональних даних для цифрової рекламної діяльності.*

*** До 2023 року також був законний інтерес.*

3.3 Процес DPIA

Етап 9. Визначте залишкові ризики та оцініть їх

Необхідність, збалансованість, справедливість

Окрім більш формальних вимог щодо законності обробки відповідно до GDPR, таких як встановлення законної підстави або прозорості, GDPR містить набір принципів, які необхідно враховувати, щоб забезпечити загальну законність обробки.

Уся робота з оцінювання за цими принципами повинна безвідмовно виконуватися на попередніх етапах. Тепер озирніться назад і зробіть остаточну оцінку вашої роботи.

- Чи необхідна обробка для досягнення цілей чи існують інші засоби, які передбачають менше втручання?
- Чи існують альтернативні засоби для досягнення цілей?
- Чи ретельно ви застосовували методи мінімізації даних і PBD?
- Чи ретельно ви впровадили методи зниження ризику для управління залишковим ризиком?
- Якщо ви йшли на компроміси на користь використання більшої кількості персональних даних або більш інтрузивної обробки, як ви виправдовуєте ці компроміси і чому вони були необхідні?
- Як залишковий ризик пропорційний перевагам обробки?
- Наскільки повідомлення суб'єктам даних, незалежно від TCF, інформує користувача про характер обробки?
- Чи дійсно користувач може зрозуміти наслідки обробки?
- Чи консультувалися ви з суб’єктами персональних даних або іншими зацікавленими сторонами?
- Чи можете ви реалізувати права суб'єктів даних щодо цих персональних даних і їх обробки?
- Як ви обґрунтовуєте терміни зберігання всіх персональних даних?
- Як ви забезпечите безпеку персональних даних і їх обробку?
- Які ваші заходи для забезпечення безперервного дотримання цього DPIA та запобігання зловживанню персональними даними, тобто поступовому розширенню обробки?

Цей аналіз дуже тонкий, тому існує багато різних інструкції та посібників на цю тему. Їх можна знайти в розділі ресурсів. Вам слід проконсультуватися з вашою DPO та іншими спеціалістами з конфіденційності.

Як пояснювалося раніше в цьому посібнику (наприклад, у розділі «Огляд процесу та етапів», сторінки 8-10), якщо залишаються будь-які високі залишкові ризики, які ви не можете зменшити, ви повинні проконсультуватися зі своїм НО перед початком обробки.

3.3 Процес DPIA

Етап 10: Підтримка вашого DPIA

DPIA створює постійне зобов'язання. Ви повинні переконатися, що ваш аналіз залишається вірним. Досягти цього можна оновлюючи контекст обробки та проводячи повторну оцінку, коли відбуваються якісь зміни.

Ви також маєте переконатись, що завжди дотримуєтесь конфіденційності (приватності), мінімізації персональних даних і заходів щодо запобігання або зниження ризиків.

Ваша DPIA для будь-якого конкретного продукту чи діяльності не є одноразовою вправою, і ви повинні переконатися, що ви переглядаєте та оновлюєте її за необхідності, відображаючи будь-які зміни в цілях, контексті, ризиках тощо.

Ви також повинні переконатися, що ваші засоби контролю та заходи щодо запобігання або зниження ризиків залишаються ефективними на постійній основі.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.4 Консультації із зацікавленими сторонами

GDPR визначає, що включає DPIA, а у ст. 35(9) говориться: У відповідних випадках контролер запитує думку суб'єктів даних або їхніх представників щодо передбачуваної обробки без шкоди для захисту комерційних чи громадських інтересів або безпеки операцій з обробки. Ви повинні розглянути цю вимогу та врахувати, чи підходить вона для відповідної обробки/продукту.

Деякі НО, такі як ICO, мають інструкції DPIA з розділом про консультації: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-adpia/#how7.

Для adtech компаній консультуватися безпосередньо з суб'єктами персональних даних не є загальноприйнятою практикою, й існують правові причини, чому залучення суб'єктів даних до процесу розробки продукту є неможливим. Замість цього може бути доречним проконсультуватися з їхніми представниками.

Існує величезна кількість загальнодоступної інформації у формі опитувань, статей, публікацій регуляторів тощо, яка демонструє погляди на природу та наслідки обробки персональних даних у галузі. Компанії повинні бути в курсі цих перспектив і чітко включати їх у свої DPIA, особливо якщо ви вирішили не консультуватися безпосередньо.

Крім того, компанії можуть подумати про те, як зібрати більше відгуків суб'єктів даних, щоб включити їх до своєї DPIA, особливо щодо використання певної обробки або типів персональних даних, які можуть бути неправильно відображені в загальнодоступних перспективах. Існує багато неурядових організацій із захисту конфіденційності (приватності), які стверджують, що представляють інтереси суб'єктів даних, і вони можуть бути хорошими ресурсами для консультацій.

Компанії повинні документувати використання точок зору суб'єктів даних, наприклад, у формі бібліографії, доданої до процесу DPIA. Що б ви не вирішили, ви повинні пояснити свої міркування у своїй DPIA. Якщо ви безпосередньо не вимагаєте надання інформації від суб'єктів даних (або їхніх представників), вам слід зафіксувати це рішення та задокументувати своє обґрунтування.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

3.5 Рішення не виконувати DPIA

Як зазначено вище, ми дотримуємося позиції – без попереднього визначення того, що вся обробка персональних даних в галузі несе високий ризик – що виконання процесу DPIA має бути стандартом, навіть якщо немає такої явної вимоги (див. "Коли потрібен DPIA?" вище).

Якщо DPIA та PBD є вбудованими у ваші процеси розробки продукту та ваш огляд існуючих продуктів, тоді DPIA слід виконувати в звичайному порядку.

Якщо обробка не представлятиме високого ризику для суб'єктів даних, тоді DPIA буде відносно легкою. Тим не менш, можуть бути випадки, коли DPIA не вимагається законом, і коли ви визначите, що вона не є необхідноюм. Краще задокументувати своє рішення не проходити DPIA та вказати причини.

"Контролер також повинен задокументувати своє обґрунтування того, чому він не запитує думку суб'єктів даних, якщо він вирішить, що це недоцільно, наприклад, якщо це поставило б під загрозу конфіденційність бізнес-планів компаній або якщо це невідповідно або неможливо."

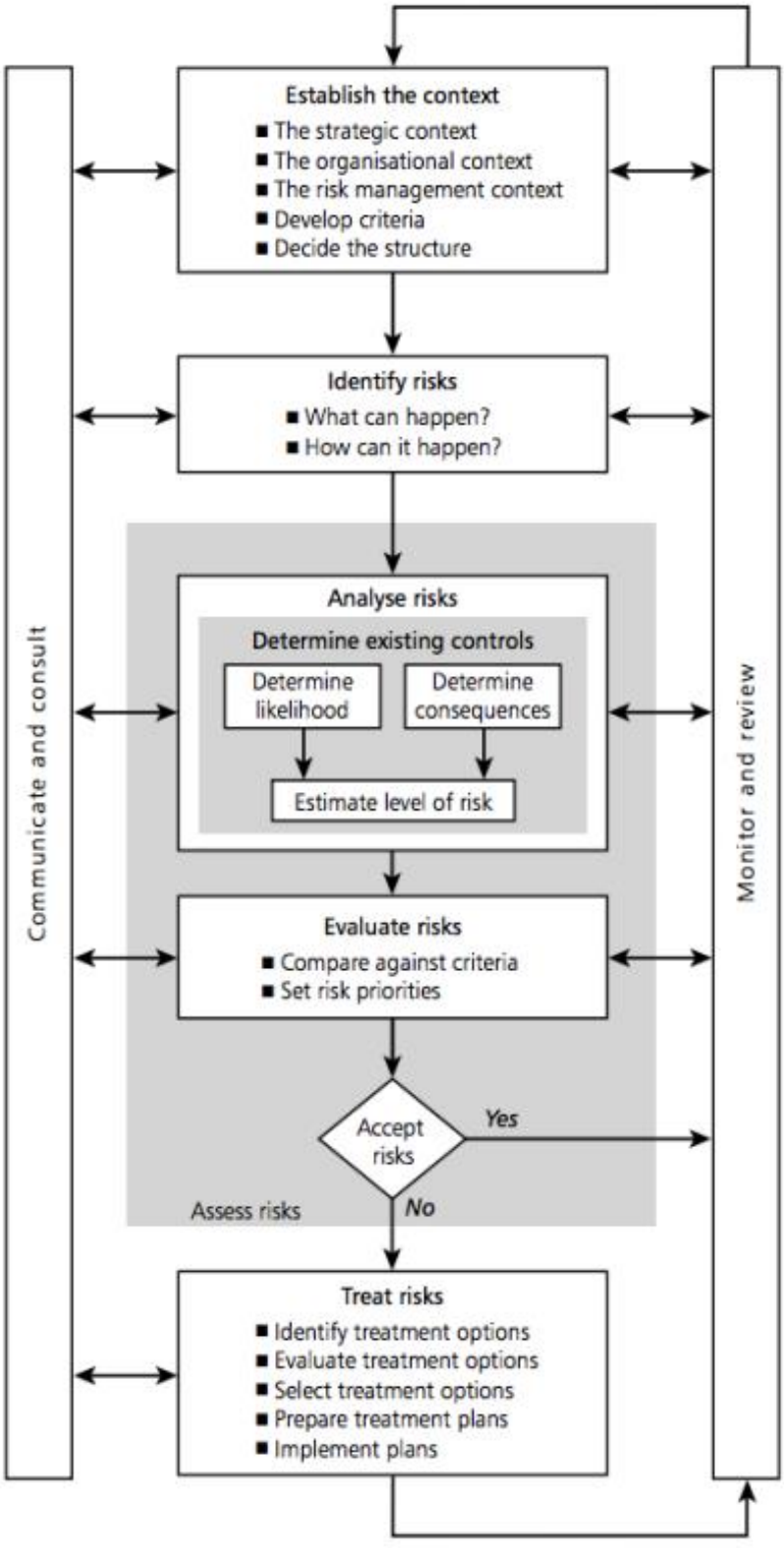
Керівництво EDPB, с. 15. 26 "У більшості випадків можна проконсультуватися з окремими особами в тій чи іншій формі. Однак, якщо ви вирішите, що це недоречно, вам слід записати це рішення як частину вашого DPIA з чітким поясненням. Наприклад, згідно з ICO, ви можете продемонструвати, що консультації можуть поставити під загрозу комерційну таємницю, конфіденційність, підірвати безпеку або бути невідповідними або неможливими.“

https://ico.org.uk/fororganisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/dataprotection-impact-assessments-dpias/how-do-we-do-a-dpia/#how7

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

Додаток А: Оцінка ризиків

Нижче наведено запропонований підхід до управління організаційними ризиками, але ту саму методологію можна застосувати в контексті DPIA, що зосереджується на ризиках для прав і свобод суб'єктів даних. Малюнок 1: Процес управління ризиками, передруковано з Standards Australia: Інструкції з управління ризиками



Додаток А: Оцінка ризиків

a) Встановіть контекст. Встановіть стратегічний, організаційний і галузевий контекст. Які дані ви обробляєте? Які категорії персональних даних? Чи є якісь дані конфіденційними, приватними чи спеціальними? [Етап 3 вашого DPIA]
b) Визначте ризики. Подумайте про інформаційні ризики, з якими стикається ваша організація. Що може статися з даними, які ви обробляєте? Чому? [Етап 5 вашого DPIA]
в) Проаналізуйте ризики. Проаналізуйте ризики з точки зору наслідків і ймовірності, щоб розрахувати рівень ризику. Цей крок докладно описано нижче. [Етап 5 вашого DPIA]
d) Оцінка та робота над ризиками. Розставте ризики за пріоритетністю та вирішіть, чи прийнятний для вас рівень ризику, з яким стикнеться організація. Для вищих рівнів ризиків розробіть план зменшення ризиків і реалізуйте проєкти, щоб забезпечити їх зменшення. [Етапи 6, 7 і 8 вашого DPIA]
д) Звіт. Якщо деякі з ризиків все ще залишаються високими після вжиття заходів щодо їх запобігання або зниження, ви повинні проконсультуватися з відповідним наглядовим органом перед початком обробки персональних даних. [Етап 9 вашого DPIA]

Аналіз ризиків: розрахунок рівня ризику
Рівень ризику визначається множенням ймовірності несприятливої події на тяжкість її наслідків.
Ризик = Ймовірність ризику x Серйозність наслідків

Як визначити ймовірність
Ви повинні прийняти обґрунтоване рішення щодо ймовірності певного ризику на основі:

- Вашого розуміння можливих причин події. Ви повинні запитати себе:

- Чому може статися ця подія?
- Які основні проблеми можуть спричинити це?
- Що може бути каталізатором/тригером події?
- Як розгорнеться ризик?
- Хто відповідальний за цей ризик?

- Ви повинні оцінити всі попередні події. Можливо, вам знадобиться перевірити попередні інциденти у вашій організації або отримати інформацію від більш широких зацікавлених сторін.

- Чи траплялась ця подія в минулому?
- Як часто? Наприклад, ви можете дослідити, скільки разів у вашій організації та в ширшому колі за останній місяць/рік/десятиліття повідомлялося про несанкціонований доступ до персональних даних через такий тип проблеми. Ви можете використати шкалу оцінки ймовірності, щоб отримати кількісну оцінку.

Шкала оцінки ймовірності

	Шкала оцінки ймовірності				
	Дуже малоймовірно	Малоймовірно	Ймовірно	Дуже ймовірно	Майже гарантовано
Descriptor	Ймовірно, це станеться за виняткових обставин	Це малоймовірно, хоча певна можливість, що це може статись, існує	Може статися і деколи траплялося раніше. Існує ймовірність	Ймовірно що це станеться	Це відбувається часто / в більшості випадків. Це скоріше трапиться, ніж ні

Як визначити наслідки.
Визначаючи ймовірні наслідки події та їх серйозність, використовуйте розумно передбачуваний найгірший сценарій. Наслідки змінюватимуться залежно від обставин, зокрема характеру ризику та типу персональних даних, що обробляються. Крім розгляду впливу на суб'єктів даних, ви повинні враховувати кількість суб'єктів даних, яких це стосується. Обробка, яка потенційно може вплинути на багато тисяч суб'єктів даних, навіть якщо вплив помірний, цілком може становити високий ризик. Ви повинні враховувати масштаб ризику та модулювати свою оцінку ризику на основі цього.
Наприклад:

	Тяжкість наслідків				
Тип/дескриптор контексту	Майже неіснуюча	Незначна	Помірна	Значна	Дуже значна
Конфіденційність суб'єкта Наприклад, внаслідок розголошення конфіденційної або чутливої інформації	Незначна шкода для суб'єкта	Незначна шкода без істотного шкідливого впливу на людину.	Помірна шкода, наприклад шкода особистим стосункам і соціальному становищу.	Велика шкода, наприклад викрадення документів з потенційними негативними наслідками	Надзвичайна шкода, наприклад, викрадення документів з фінансовими втратами, втратою роботи, ризиком для життя чи здоров'я.

Додаток В:
Приклади персональних даних, ризики та заходи щодо запобігання або зниження ризиків У таблиці нижче описано персональних дані, які зазвичай використовуються в цифровому маркетингу, ризики, які можуть виникнути внаслідок обробки цих даних, а також можливі засоби контролю та пом'якшення цих ризиків. Вони призначені як джерело натхнення та спроба створити певне узгодження у галузі навколо цих питань. Цей список аж ніяк не є вичерпним чи повним. Вам потрібно буде звернутись до зовнішніх ресурсів і ваших внутрішніх фахівців з конфіденційності (приватності), щоб врахувати всі нюанси.

Примітка: щодо конфіденційних або потенційних персональних даних особливої категорії, як визначено статтею 9 GDPR, ми припускаємо, що такі дані не навмисно обробляються для цілей цифрової реклами. Однак можливо, що обробка персональних даних неспеціальної категорії може призвести до ризику обробки даних спеціальної категорії, залежно від того, що це за дані, як вони використовуються та з якою метою. Цей ризик може бути актуальним для певних типів даних, наприклад, історії веб-перегляду, сегментів інтересів, місцезнаходження та точної геолокації. Слід пам'ятати про ненавмисну обробку персональних даних спеціальної категорії та запобігати їй. IAB UK підготував спеціальні вказівки щодо персональних даних спеціальних категорій:

Тип даних	Опис	Примітки про ризики	Мінімізація, PBD та міркування щодо зменшення ризику
Ідентифікатори	Це різні типи ідентифікаторів, які зазвичай використовуються в галузі. Усі вони можуть вважатися персональними даними	Будь-який ідентифікатор може полегшити повторну ідентифікацію псевдонімізованих даних. Існує ризик того, що ідентифікатор, який спочатку не призначений для безпосередньої ідентифікації, стане таким через зіставлення ідентифікаторів.	Використання псевдонімізованих даних є технікою PBD. Це може зменшити ризик повторної ідентифікації та комбінування наборів даних. Солоні хеші можуть покращити захист від цих ризиків. Однак майте на увазі, що псевдонімізовані дані все ще є особистими та містять ризик повторної ідентифікації. Просте хешування ідентифікаторів не є надійним засобом деідентифікації даних. Також зауважте, що необхідно остерігайтися відомих вразливих алгоритмів хешування, таких як MD5 або SHA1. Термін життя ідентифікаторів і ідентифікованих даних має бути якомога коротшим. Видаліть ідентифікатори з даних якомога швидше.
- Псевдонімізовані ідентифікатори	Псевдонімізовані ідентифікатори, такі як IP-адреса, файли cookie та ідентифікатори пристроїв.		Дивись вище. Зауважте, що скорочену IP-адресу необов'язково вважати неособистою; це залежить від контексту
- Псевдонімізовані ідентифікатори, наприклад хешована адреса електронної пошти	Псевдонімізовані ідентифікатори, отримані з прямих ідентифікаторів, включаючи, наприклад, хешовану адресу електронної пошти	Остерігайтеся ризиків повторної ідентифікації у ваших руках або в руках одержувачів даних. Чи можна дані, зібрані під псевдонімом за цими ідентифікаторами, повторно співвіднести з основним прямим ідентифікатором?	Дивись вище. Як зазначалося вище, хешування має обмеження. Отже, хоча хешування адреси електронної пошти (або іншого прямого ідентифікатора) покращує конфіденційність (приватність), пам'ятайте, що ці дані є вразливими до атаки веселкової таблиці. Крім того, існують способи збереження одностороннього збігу, щоб запобігти повторній кореляції даних, які були зібрані під псевдонімом, із прямим ідентифікатором
- Імовірнісна ідентифікація пристрою	Синтетичні недетерміновані ідентифікатори, отримані з імовірнісних моделей і/або моделей машинного навчання з використанням таких вхідних даних, як IP-адреса, агент користувача та інші характеристики мережі, пристрою чи браузера.	Імовірнісні ідентифікатори є непрозорими, і суб'єкту даних їх важче контролювати, ніж детерміновані ідентифікатори.	Прозорості та контролю важко досягти. З іншого боку, неточність або «нечіткість» ідентифікації можна вважати корисною для конфіденційності (приватності). Наскільки точність і чіткість вам потрібні для ваших цілей?

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

Тип даних	Опис	Примітки про ризики	Мінімізація, PBD та міркування щодо зменшення ризику
- Прямі ідентифікатори	Непсевдонімізовані ідентифікатори, такі як адреса електронної пошти, ім'я користувача, номер рахунку. Вони стають все більш поширеними в промисловості	Історично більшість даних, зібраних у галузі, були під псевдонімами. Люди часто кажуть: «Ми не знаємо і не хвилюємося, хто ви, усе, що у нас є, — це ідентифікатор файлів cookie.» Однак із використанням більш прямих ідентифікаторів існує підвищений ризик, наприклад, повторної ідентифікації історії веб-перегляду. який спочатку було зібрано за допомогою файлу cookie.	Замість цього використовуйте псевдонімізовані ідентифікатори, якщо можливо. Зверніть увагу на підвищений ризик безпеки обробки цих даних. Також врахуйте, що обробка цих даних може призвести до більш широких зобов'язань щодо виконання прав користувачів, оскільки вони з'єднують більше даних і є більш постійними.
Історія веб-перегляду або використання програми	Запис, незалежно від того, призначений чи ні, онлайн-активності суб'єктів даних. Зауважте, що щось на кшталт журналів веб-сервера, що записують піксельні виклики синхронізації, відповідатиме вимогам. Справа в тому, що онлайн-активність конкретного користувача або пристрою можна реконструювати за даними	Ці дані можуть розповісти багато про суб'єкта даних, у тому числі деякі дуже особисті речі. Крім того, загальноприйнято розуміти, що відчуття стеження заважає вільному висловлюванню.	Видаліть або належним чином деідентифікуйте історію якомога швидше. Розгляньте можливість видалення параметрів URL-адреси, шляхів до каталогу та іншої інформації як тимчасового заходу для зменшення інформації.
Сегменти інтересів	Категорії інтересів, як би не були похідними.	Сегменти можуть розкривати особисту інформацію, а іноді можуть використовуватися для небажаного впливу на суб'єкта даних (див. Додаток С).	Обмежте тривалість життя на сегментах. Регулюйте, які сегменти дозволені. Розгляньте прозорість конкретних сегментів, які ви використовуєте.
Демографічна інформація	Інформація про демографічні характеристики суб'єкта даних.	Те саме, що сегменти. Остерігайтеся ризику дискримінаційного використання цієї інформації	

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

Тип даних	Опис	Примітки про ризики	Мінімізація, PBD та міркування щодо зменшення ризику
Точна геолокація	Немає законодавчо визначеного порогу для точного проти неточного; однак поточна політика TCF вважає дані неточними, якщо вони точні в радіусі понад 500 метрів і/або для координат GPS мають два або менше знаків після коми	Ці дані можуть відображати фізичну поведінку суб'єкта даних і можуть включати деяку дуже конфіденційну інформацію, таку як відвідування медичних установ або місць відправлення культу. Слід враховувати щільність населення. Точна географія в місті має інші наслідки для конфіденційності (приватності), ніж у сільській місцевості.	Ви можете зменшити точність GPS-координат, опустивши десяткові знаки або перетворивши їх на поштовий індекс, назву міста чи іншого більшого географічного регіону. Вам слід розглянути можливість підвищення географічного рівня до територій з мінімальною щільністю населення. Існують різні способи зробити це. Будьте обережні з конфіденційними (приватними) місцями, такими як школи, церкви, медичні установи, державні установи тощо. Будьте особливо обережні, надаючи ці дані
Неточна геолокація	Дивіться вище точну геолокацію	Навіть у неточному вигляді геолокаційні дані можуть виявити конфіденційну інформацію. Наприклад, показати, що хтось був у місті чи районі, де його не очікували, або піддати когось підозрі через те, що він був неподалік від злочину.	Як зазначалося, неточне геолокування пов'язане з ризиком для конфіденційності (приватності). Примітка про точне географічне розташування та щільність населення також застосовується і тут.
Географічні сегменти	Сегменти, засновані на фізичній поведінці суб'єктів даних, наприклад, "пішли в продуктовий магазин», «пішли в Sainsbury's» або «пішли в Waterloo Sainsbury's».	У більш абстрактній формі сегментів ця геоінформація може виявити дані, які людина вважатиме дуже особистими або конфіденційними (приватними). Вони не мають таких же характеристик конфіденційності (приватності), як сегменти інтересів, отримані з поведінки в Інтернеті.	Здійснюйте контроль над дозволеними сегментами.
Дата та час вищевказаного	Інформація про дату й час, пов'язана з інформацією про поведінку, описаною вище.	Це показує, що хтось робив у певний час, іноді в певному місці. Наприклад, вони сиділи в Інтернеті в кафе, коли стверджували, що сплять вдома.	По можливості видаліть мітки часу. В іншому випадку зменшіть точність. Вам потрібні секунди, коли достатньо годин? А як щодо частин доби чи днів? тижні?
Інформація про пристрій	Така інформація, як марка, модель, версія пристрою або браузера, а також налаштування та можливості пристрою тощо. Усі ці характеристики можуть полегшити розрізнення пристроїв або користувачів і часто використовуються як критерії націлювання самостійно.	Чим детальнішою є ця інформація, тим більший ризик того, що її можна використовувати для розрізнення користувачів і пристроїв	Знизьте точність якомога більше. Наприклад, вам потрібен номер збірки браузера чи достатньо типу браузера?

Тип даних	Опис	Примітки про ризики	Мінімізація, PBD та міркування щодо зменшення ризику
Граф між пристроями	Співвідношення пристроїв, якими володіє або користується один користувач	Графи для різних пристроїв, як правило, непрозорі. Існує ймовірність збентеження або гіршого, оскільки поведінка на одному пристрої впливає на рекламу на іншому. Подумайте, наприклад, про покупку обручки або про розлучення. Також існує ризик зв'язування більшої кількості даних – даних, пов'язаних з різними пристроями, можливо, даних, які користувач сподівався зберігати окремо. Подумайте про роботу чи особисті пристрої.	З усіма даними графа будьте обережні, надсилаючи граф особливо в поєднанні з ідентифікаторами пристроїв. Ви можете поділитися даними, які, на вашу думку, надійшли від одного користувача чи родини, не розкриваючи конкретних пристроїв. Розгляньте засоби контролю способів використання цих даних, беручи до уваги можливість витоку даних крос-графа. Наприклад, певні категорії оголошень можуть бути неприйнятними.
Граф домашнього господарства	Співвідношення пристроїв, якими володіють або користуються користувачі в одній родині.	Існує ризик того, що кореляція домашніх пристроїв призведе до того, що дані про одного користувача в домогосподарстві будуть розкриті іншим користувачам.	Дивись вище.
Соціальний граф	Співвідношення користувачів, які, як вважають, взаємодіють один з одним соціально.	Це може бути конфіденційна (приватна) інформація, особливо якщо користувач явно не розкрив цю інформацію. Соціальні зв'язки людей можуть багато про них розповісти. Крім того, ця кореляція може звести нанівець спроби користувача відокремити соціальні асоціації. І, як і у випадку з графами домогосподарств, існує ризик розкриття інформації про одного користувача на графу іншим користувачам на графіку	Дивись вище.
Конфіденційні (приватні) дані або дані спеціальної категорії	Дані про дітей або дані, які можуть підпадати під одну або декілька спеціальних категорій статті 9.	Навіть якщо ви не збираєтеся збирати ці дані та не ідентифікуєте їх, часто існує ризик, що ви можете це зробити, або що це може виникнути через те, як інші дані (наприклад, місцезнаходження, історія веб-перегляду) зберігаються та використовуються .	Ви повинні вжити заходів, щоб уникнути випадкового збору цих даних. Наприклад, це може означати контроль ваших джерел даних або це може означати розпізнавання даних, коли вони надходять у вашу систему, а не записування їх в особистій формі.
Онлайн-офлайн зіставлення	Зіставлення ідентифікаторів з метою кореляції поведінки в режимі офлайн і онлайн або, загалом, між різними контекстами. Наприклад, зіставлення записів про онлайн-рекламу, яку переглядають, з історією покупок користувача у роздрібного продавця/рекламодавця.	Це зіставлення створює ризик повторної ідентифікації та кореляції даних у різних контекстах у спосіб, якого суб'єкт даних не очікує.	

Зауважте, що деякі з наведених вище категорій зазвичай використовуються як компоненти в іншій обробці, але можуть вимагати створення окремої DPIA. Наприклад, побудова діаграми різних пристроїв або домогосподарств повинна мати DPIA.

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

Додаток C: Загальні ризики в індустрії цифрової реклами

Це неповний перелік поширених ризиків, пов'язаних із діяльністю обробки в індустрії цифрової реклами, з деякими міркуваннями щодо кожного. Він надається як корисна довідка. Вам слід уважно подумати про ризики, наявні у ваших обставинах, які тут можуть бути не представлені. Для власного DPIA вам потрібно буде проаналізувати вплив і ймовірність конкретних ризиків, які ви ідентифікуєте (див. основні вказівки). Деякі типи ризиків, якщо вони справдяться, ніж інші, матимуть більш шкідливий вплив на суб'єктів даних і ви повинні взяти це до уваги під час аналізу.

Розгляд ризиків

Ризик	**Міркування**
Очікування та права суб'єкта даних	
суб'єкт даних не очікує обробки	суб'єкти даних очікують цю обробку персональних даних чи вони будуть здивовані? Конкретні речі, які можуть викликати здивування, включають, наприклад, обробку в, здавалося б, непов'язаних контекстах, зіставлення даних із різних джерел, на різних пристроях, у різних домогосподарствах і соціальних мереж. Надання достатньої інформації та прозорість обробки може допомогти гарантувати, що суб'єкти даних не будуть здивовані.
Ніяковість	Чи може суб'єкт даних почуватися ніяково якщо, наприклад, він отримає рекламу на делікатну тему, засновану на його веб-переглядах? Що, якщо хтось інший побачить рекламу або вона відображатиметься на інших пристроях?
Небажане розголошення	Чи можуть дані про суб'єкта даних розкриватися іншим сторонам у такий спосіб, який не влаштує і здивує суб'єкта даних? Наприклад, чи можна зіставити історію веб-переглядів з даними CRM продавця?
Дискомфорт – відчуття втручання у приватне життя	Користувачі можуть відчувати дискомфорт через певну обробку персональних даних, коли вони дізнаються про неї. Наприклад, багато користувачів відчувають дискомфорт, коли відбувається ретагретинг. При оцінці впливу ризику слід враховувати рівень втручання в конфіденційність (приватність) користувача
Перешкода самовираження	У зв'язку з вищесказаним існує занепокоєння, що коли онлайн-користувачі відчувають, що за ними спостерігають, вони менше виражають себе онлайн. Наприклад, чи можуть вони бути менш схильні досліджувати свій стан здоров'я або спілкуватися з іншими користувачами з подібними політичними переконаннями, якщо вони хвилюються, що за їх поведінкою спостерігають?
Недотримання прав суб'єктів даних	Будьте обережні щодо дотримання прав суб'єктів даних. Природа даних і обробка в галузі інколи створює проблеми з дотриманням цих прав. Продумайте, коли і як ви дотримуєтеся прав суб'єктів даних і де виникають проблеми; спробуйте знайти баланс, який буде вигідним для суб'єкта даних і в межах духу (а також букви) закону

Джерело:https://iabeurope.eu/wp-content/uploads/2020/11/IAB-Europe_DPIA-Guidance-Nov-2020.pdf

Ризик	Міркування
Справедливість і дискримінація	
Неправомірний вплив на вразливі верстви населення	Чи можна використовувати дані для виявлення вразливих груп населення, щоб впливати на них або використовувати їх? Наприклад, чи можна використати інформацію про доходи або дані веб-пошуку, щоб ідентифікувати людей із фінансовими проблемами та постійно пропонувати їм кредити? Подібним чином люди похилого віку часто стають уразливими, і з'являється ймовірність, що ними можуть скористатися: демографічна інформація може бути використана, щоб ідентифікувати їх в Інтернеті.
Втручання у політику	Що стосується занепокоєння стосовно впливу на вразливі верстви населення, то минулі вибори показали, як можна використовувати дані для сегментації та мікроцільових меседжів для певних груп населення, часто для розпалювання ворожнечі та/або поширення дезінформації. Зокрема, демографічні дані, дані про політичні інтереси та дані про місцезнаходження вразливі до використання таким чином. Примітка: персональні дані, що розкривають політичні погляди, є чутливими (даними особливої категорії відповідно до ст. 9 GDPR), які не можуть бути оброблені, якщо не застосовуються/ дотримуються певні особливі умови. Для цілей цього посібника ми припускаємо, що навмисної обробки персональних даних спеціальної категорії не відбувається. Однак ви повинні знати про ризик ненавмисної обробки чутливих персональних даних (персональних даних спеціальної категорії) та зменшити його.
Вплив на придатність або доступність продукту чи послуги, наприклад, страховка, фінанси тощо	Чи можуть дані використовуватися, щоб вплинути на право на отримання кредитів, страхування чи інших продуктів і послуг? Зауважте, що способи вибору аудиторії для певної реклами потенційно можуть використовуватися в дискримінаційний спосіб. Наприклад, інформацію про місцезнаходження можна використовувати, щоб запобігти показу реклами кредитів у певних районах
Вплив на зайнятість	Чи можуть дані вплинути на пропозиції про роботу не тільки в тому, чи отримає хтось роботу чи ні, але навіть у тому, чи побачать вони оголошення про вакансію чи ні?
Уразливі групи	
Обробка персональних даних вразливих груп, наприклад дітей	Хоча ви, можливо, цього робити не збираєтеся, ви можете ненавмисне обробити персональних дані дітей. Ми не кажемо вам ідентифікувати дітей, але можливо ідентифікувати та відфільтрувати дані, які можуть вказувати на те, що суб'єкт даних є дитиною. Наприклад, ви можете ідентифікувати веб-сайти, призначені для дітей, і обробляти дані з цих сайтів по-іншому, наприклад, не зберігаючи дані в особистій формі.
Безпека даних і обмін даними	
Порушення та зловживання даними	Навіть псевдонімізовані дані несуть за собою такі ризики як витік даних або інший ненавмисний доступ до даних.
Неправомірне використання персональних даних законним власником (як порушення договору чи іншим чином)	Коли ви надаєте співробітникам доступ до персональних даних або ділитеся даними з іншими сторонами, існує ризик того, що вони зловживатимуть цими даними. Ви повинні мати засоби безпеки та контролю доступу, а також відповідну політику, а також переконатися, що ця політика є ефективною та що її дотримуються на постійній основі. Договірні обмеження під час обміну персональними даними корисні, але цього недостатньо. Використовуйте технічні обмеження, коли це можливо, і встановіть процедури для моніторингу відповідності/примусового виконання, якщо ви повинні покладатися на контракти. Див. окреме керівництво після публікації.
Невідповідність операторів	GDPR вимагає наявності певних договірних положень із операторами даних. Ви, як контролер, несете відповідальність за моніторинг/забезпечення їх дотримання. Оператори є ще одним вектором, де може статись порушення або витік персональних даних і неправомірне використання персональних даних. Використовуйте технічні обмеження, тобто мінімізуйте персональні дані, які ви надаєте оператору, і користуйтеся своїми правами на моніторинг/аудит відповідності операторів.
Доступ з боку правоохоронних органів або іншого судового процесу	Збір даних комерційними організаціями може вплинути на законні права суб'єктів даних різними способами, включно з можливістю доступу до них правоохоронними органами та іншими кримінальними чи цивільними судовими установами. Ви, звичайно, повинні дотримуватися закону, але ви можете вжити заходів, щоб зменшити цей ризик. Можна мінімізувати або видалити дані. Ви також можете переконатися, що такі юридичні запити є обґрунтованими, а не надмірними. Використовуйте доступні вам правові механізми для захисту прав суб'єктів даних, чиїми даними ви володієте.
Повторна ідентифікація псевдонімізованих даних	Дані в галузі часто збираються та обробляються під псевдонімом. Зазвичай ми вважаємо меншим ризик для конфіденційності, якщо ми не знаємо справжню особу суб'єкта даних. Однак у багатьох випадках у галузі повторно ідентифікувати дані та зіставити їх із справжньою особистістю нескладно. Це може статися значно пізніше, не одразу після збору даних, і сторони, залучені до початкового збору, включно з суб'єктом персональних даних, можливо, на той час не очікували, що дані коли-небудь будуть безпосередньо ідентифіковані. Після повторної ідентифікації даних ризики зростають.

Конфіденційність (приватність) і захист персональних даних

Зміст

Прецедентне право Суду Європейського Союзу (Суду ЄС)

"Суд Європейського Союзу (далі по тексту Суд ЄС) є найвищим судом, який приймає рішення з питань матеріального права. Оскільки GDPR є регламентом ЄС, це означає, що тлумачення закону Суду ЄС є остаточним.

Незважаючи на те, що GDPR є всеосяжним законом, який має однаково застосовуватися в усьому ЄС, його виконання контролюють регулятори на національному рівні.

Це означає, що деякі поняття, такі як згода та законний інтерес, можуть тлумачитися по-різному залежно від країни-члена ЄС. Таким чином, рішення Суду ЄС допомагають більш детально зрозуміти, як GDPR має застосовуватися та перевірятися, і можуть допомогти обґрунтувати певні методи захисту персональних даних.

Джерело: https://iabeurope.eu/privacy-data-protection/

Нормативно-методичні документи

Як ми згадували вище, виконання GDPR залежить від наглядових органів національного рівня. На жаль, вони не завжди згодні щодо того, як слід тлумачити певні положення закону, і це особливо вірно, коли йдеться про те, як вони мають намір забезпечити виконання правил у випадках використання онлайн-реклами.

Ми підготували невелику таблицю, яка висвітлює деякі різні тлумачення законодавства наглядовими органами в їхніх керівних документах, а також посилання на керівні сторінки або документи.

Джерело: https://iabeurope.eu/privacy-data-protection/

e-Privacy Директива та GDPR

GDPR – не єдине законодавство ЄС у сфері конфіденційності та захисту персональних даних. Насправді e-Privacy Директива, яка головним чином зосереджена на забезпеченні конфіденційності в телекомунікаційному секторі, містить особливе положення (стаття 5(3)), яке вимагає отримання згоди на доступ або зберігання інформації на пристрої користувача, включаючи файли cookie та інші пристрої використовується технологією онлайн-реклами для різних цілей (таких як аналіз аудиторії, націлювання, перевірка реклами та безпека). Це означало, що директиву також часто називали «законом про файли cookie».

- Визначення згоди в e-Privacy Директиві взято з GDPR, тобто ті самі вимоги застосовуються до отримання згоди на розміщення файлів cookie (або подібних технологій) або доступу до інформації з пристрою. Однак e-Privacy Директива не розрізняє персональні та неперсональні дані, тобто сама дія доступу до інформації або збереження інформації на пристрої викликає вимогу згоди, незалежно від характеру цієї інформації.

- У статті 95 GDPR визнається, що e-Privacy Директива є тим, що називається «lex specialis» — більш конкретним законом, який має перевагу над GDPR у сфері його застосування. Це, по суті, означає, що там, де застосовується e-Privacy Директива, вона встановлює більш конкретне правило, а саме, для зберігання чи доступу до інформації на чиємусь пристрої лише згода може використовуватися як правова основа, і не має значення, чи є ця інформація персональними даними, чи ні.

Оскільки e-Privacy Директива є старішим законом, який спочатку набув чинності в 2002 році та отримав оновлення в 2009 році, також були спроби прийняти нову версію - e-Privacy Регламент. Цей процес все ще триває, і якщо ви хочете дізнатися більше про адвокаційні зусилля IAB Europe, ви можете знайти більше інформації на сторінці Європейської цифрової політики IAB Europe.

Джерело: https://iabeurope.eu/privacy-data-protection/

ЄС-США Оит конфіденційності (приватності) (EU-US Privacy Shield)

16 липня 2020 року Суд ЄС у своєму рішенні у справі C-311/18 (Schrems II) визнав недійсним Щит конфіденційності (приватності) між ЄС і США. Це Рішення безпосередньо стосується будь-якої компанії, яка використовувала Оит конфіденційності (приватності) для передачі персональних даних із ЄС до США, і має ширші наслідки щодо законності передачі персональних даних за допомогою стандартних договірних положень (Standard Contractual Clauses - «SCC») будь-якій не-країні ЄС. Це вже другий раз, коли Суд ЄС визнав недійсним механізм передачі даних; у 2015 році принципи безпечної гавані (Safe Harbour principles) також були визнані недійсними Судом ЄС у справі C-362/14 (Schrems I) за відносно схожих обставин.

На сторінці із поширеними запитаннями про Оит конфіденційності (приватності) між ЄС та США IAB Europe підсумув, що це рішення означає для онлайн-рекламиии, яких пасток слід уникати та де шукати докладніші вказівки.

Джерело: https://iabeurope.eu/privacy-data-protection/

TCF&CMPs

Протокол Прозорості та Згоди

і

Платформи Адміністрування Згоди

Зміст

Що таке Протокол Прозорості та Згоди (ППЗ)/Transparency & Consent Framework (TCF)?

Протокол Прозорості та Згоди (ППЗ) /Transparency and Consent Framework або TCF (“Протокол прозорості та згоди”) від IAB Europe — це єдине рішення для отримання згоди кінцевого користувача відповідно до GDPR, що виконує роль стандарту в індустрії.

Мета ППЗ/TCF полягає в тому, щоб допомогти всім учасникам ланцюжку цифрової реклами переконатися, що вони дотримуються GDPR та e-Privacy Директиви

ППЗ/TCF створює середовище, у якому видавці веб-сайтів можуть інформувати користувачів щодо збору персональних даних таких суб’єктів та цілі їх використання не лише самим власником таких веб-сайтів (Першою особою), але і партнерами, з якими він співпрацює (Третіми особами). ППЗ/TCF надає видавничій та рекламній галузям «спільну мову», за допомогою якої можна повідомляти про згоду користувачів на показ відповідної онлайн-реклами та контенту.

ППЗ/TCF v1.1 було запущено 25 квітня 2018 року після широких галузевих консультацій з членами IAB Europe та IAB Tech Lab, а також з індустрією цифрової реклами в цілому. 21 серпня 2019 року було запущено переглянуту версію ППЗ/TCF v2.0, що використовується й зараз. Впровадження оновленої версії ППЗ/TCF v.2.2 очікується до кінця вересня 2023 року.

Джерело: https://iabeurope.eu/transparency-consent-framework/

TCF для видавців

Видавець — це оператор (власник) веб-сайту, додатку чи іншого контенту, де відображається цифрова реклама або збирається чи обробляється інформація про користувачів з метою демонстрації цифрової реклами, вимірювання, аналітики або персоналізації контенту.

Видавці повинні прочитати та дотримуватися Політик ППЗ/TCF, зокрема Політики, що стосується інтерфейсу користувача. Цей інтерфейс забезпечує регулярне інформування користувача про мету та законну підставу обробки його персональних даних постачальниками, з якими видавці бажають працювати, в результаті відвідування таким користувачем веб-сайтів, додатків або іншого контенту.

Видавці, які дотримуються Політики ППЗ/TCF, повинні виконувати такі дії:

- Ретельно відбирати та контролювати постачальників, з якими вони хочуть працювати;
- Надавати користувачам прозорість щодо постачальників, обраних видавцем, і мети обробки персональних даних;
- Запитувати та отримувати інформовану згоду кінцевих користувачів на обробку їхніх персональних даних або обґрунтовувати інші законні підстави для обробки персональних даних;
- Прозоро передавати іншим учасникам ринку інформацію, що стосується вибору користувача;
- Або діяти як платформа адміністрування згоди (CMP). У цьому випадку їм потрібно буде зареєструватися як ПАЗ/CMP у ППЗ/TCF або користуватися послугами ПАЗ/CMP, зареєстрованої в ППЗ/TCF;
- Підтримувати використання даних для вимірювання ефективності кампанії та використання контекстної реклами, яка вимагає доступу до пристроїв користувача.

Джерело: https://iabeurope.eu/transparency-consent-framework/

TCF для рекламодавців та агенцій

Рекламодавці, як і видавці, отримують доступ до персональних даних кінцевих користувачів та є операторами веб-сайтів, які мають прямі контакти з кінцевими користувачами. Цей зв'язок може здійснюватися через веб-сайт, додаток або інший контент.

Якщо відображається цифрова реклама або інформація про користувачів збирається та використовується для цифрової реклами, вимірювання та аналітики або персоналізації контенту, оператор зобов'язаний фіксувати факт згоди користувача та переконуватись, що сигнал згоди поширюється в екосистемі постачальників, з якими веб-сайт співпрацює.

Операторам веб-сайтів треба подбати про безліч деталей, що супроводжує згоду кінцевого користувача, і в цьому стають в нагоді сервіси ПАЗ/CMP. ПАЗ/CMP надає комплексне рішення для адміністрування згоди кінцевих користувачів, що відповідає конкретним потребам таких веб-сайтів. Крім того, оператори веб-сайтів можуть стати ПАЗ/CMP і створити власне рішення для отримання згоди.

https://iabeurope.eu/tcf-for-advertisers-agencies/

https://iabeurope.eu/knowledgehub/policy/iab-europe-transparency-and-consent-framework/tcf-v2-0-support-materials-marketing-collateral/

TCF для CMP

Платформа адміністрування згоди (Consent Management Platform або ПАЗ/CMP) — це програмний комплекс, який забезпечує прозорість щодо процесу надання згоди або відмови кінцевим користувачем веб-сайту. ПАЗ/CMP може зчитувати та оновлювати законні підстави щодо збору інформації компанією, яка бере участь у постачанні цифрової реклами (зазвичай її називають постачальником) на веб-сайті видавця, у додатку чи іншому цифровому контенті. Постачальники фіксують перелік своїх законних підстав для обробки персональних даних користувачів та мету доступу до їх пристроїв чи браузерів у Глобальному списку постачальників (Global Vendor List або GVL).

ПАЗ/CMP виконує такі дії:

- Надає користувачам прозорість щодо постачальників, з якими видавець ділиться персональними даними своїх користувачів;
- Забезпечує прозорість щодо мети і законних підстав, на яких ґрунтується обробка персональних даних постачальником – назви та описи цих елементів і функцій можна знайти тут;
- Зберігає сигнали згоди користувача, наприклад файли cookie третьої особи, у браузері користувача та робить інформацію про згоду користувача доступною для постачальників у рядку ППЗ/TCF v2.0 (з жовтня 2023 - ППЗ/TCF v.2.2);
- Переконується, що у випадку, коли користувач дає згоду на збір персональних даних лише з певною метою, згода поширюється лише на постачальників, які заявили через GVL, що вони використовують дані з цією метою.
- ПАЗ/CMP повинні швидко реагувати на зміни в специфікаціях ППЗ/TCF від IAB Europe і Політиках ППЗ/TCF. Вони також повинні проходити щорічний тест ПАЗ/CMP, який перевіряє відповідність функціонування інструменту специфікаціям ППЗ/TCF і Політикам ППЗ/TCF.

ПАЗ/CMP Валідатор

ПАЗ/CMP Валідатор був розроблений IAB Europe для перевірки того, що робота ПАЗ/CMP відповідає Технічній специфікації та Політиці ППЗ/TCF. Усі CMP, які реєструються в ППЗ/TCF, повинні пройти перевірку, перш ніж їм буде видано ідентифікатор ПАЗ/CMP, який дозволить їм установити рядок ППЗ/TCF v2.0 (з жовтня 2023 - ППЗ/TCF v.2.2). ПАЗ/CMP Валідатор опубліковано у веб-магазині Chrome у приватному режимі та доступний лише для ПАЗ/CMP, які зареєстровані в ППЗ/TCF, та видавців, які використовують ПАЗ/CMP, що належним чином зареєстрована в IAB ППЗ/TCF.

TCF версії 2.2

Основні поправки до політики TCF версії 2.2

- Видалення правової основи законного інтересу для персоналізації реклами та вмісту: у рамках TCF Постачальники зможуть вибирати лише згоду як прийнятну правову основу для цілей 3, 4, 5 і 6 на рівні реєстрації;

- Покращення інформації, що надається кінцевим користувачам: змінилися назви та описи цілей і функцій. Юридичний текст видалено та замінено зручними описами, доповненими прикладами реального використання (ілюстраціями);

- Стандартизація додаткової інформації про Постачальників: Постачальники повинні будуть надавати додаткову інформацію про свої операції з обробки даних, щоб цю інформацію, у свою чергу, можна було розкрити кінцевим користувачам;
    1. Категорії зібраних даних
    2. Періоди зберігання залежно від мети
    3. Заяву про наявність законних інтересів – якщо це можливо

Прозорість щодо кількості Постачальників: CMP повинні будуть розкривати загальну кількість Постачальників, які прагнуть створити правову основу на першому рівні своїх інтерфейсів користувача;

Конкретні вимоги для спрощення відкликання згоди користувачів: видавці та CMP мають переконатися, що користувачі можуть знову відкрити інтерфейси CMP і легко відкликати згоду.

Будь ласка, ознайомтеся з відповідними розділами оновленої Політики, щоб отримати додаткові відомості, а також з дописом у блозі IAB Europe тут .

Оновлення технічних специфікацій TCF v2.2

З метою впровадження цих змін політики IAB Tech Lab оновила технічні специфікації для Transparency & Consent Framework. Ці зміни включають:

Припинення підтримки getTCData та вимога до постачальників використовувати EventListeners, де це можливо

Оновлення GVL: версія буде збільшена до 3, а GVL міститиме додаткові дані:

нові поля для таксономії категорій даних

включення періодів зберігання даних для кожної мети

підтримка багатомовного оголошення URL

Будь ласка, ознайомтеся з оновленими технічними специфікаціями для отримання додаткової інформації та публікацією в блозі IAB Tech Lab тут .

Бібліотека Javascript, яка підтримує реалізацію учасників TCF, також оновлюється для розміщення TCF v2.2 тут .

Дякуємо за співпрацю!

Якщо у вас є зауваження, пропозиції та доповнення, будь ласка повідомте нас електронною поштою
svitlana.lemeshko@iab.com.ua
Ми врахуємо усі конструктивні доповнення у наступній редакції