ЗНАЙОМСТВО З GDPR
МАЛИЙ ГАЙД

Інформаційний партнер

mgid

Вступне слово

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. Це матиме безпосередній економічний вплив на результати діяльності компанії через систему істотних штрафів за порушення норм GDPR.

Поза тим, 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 в ЄС.

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

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 застосовуватися як законодавча норма 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, 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-яка операція або низка 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 Україна на основі матеріалів Групи IAB Europe з виконання GDPR (**GIG**), щоб надати рекомендації українським компаніям по всьому світу щодо дотримання GDPR в правовій площині.

GDPR: ВИЗНАЧЕННЯ СУТЬ МЕТА

GDPR як база захисту

Олександра Булигіна
Керівник комітету Programmatic IAB Україна, Директор, Amnet, member of Dentsu Aegis Network Ukraine

Сучасний світ неможливо уявити без цифрових технологій та інтернету. Ці технології змінили спосіб, яким бізнеси спілкуються зі своїми клієнтами та просувають свої продукти чи послуги. Однак, разом із цими можливостями прийшла і проблема захисту особистих даних користувачів. Саме для регулювання цього питання і був створений Загальний регламент з питань захисту даних (GDPR) у Європейському Союзі.

У цьому вступі ми розглянемо суть і мету GDPR з фокусом на вплив цього Регламенту на рекламні технології та диджитал рекламу, яка вимагає збору та обробки величезних обсягів особистих даних користувачів.

Суть та мета GDPR

GDPR був прийнятий з метою захисту особистих даних громадян Європейського Союзу. Основною суттю цього Регламенту є надання більшого контролю особам над їхніми особистими даними та забезпечення їхньої приватності. Для досягнення цієї мети, GDPR встановлює ряд ключових принципів та обов'язків для підприємництва:

1. Забезпечення прав осіб: GDPR надає користувачам право на доступ до своїх даних, право на виправлення невірних даних, право на забування (право бути видаленим з бази даних) та інші права, що дозволяють контролювати їхні дані.

1. Обов'язки для організацій: Підприємства повинні дотримуватися правил обробки особистих даних, включаючи введення політик та процедур для забезпечення їхньої безпеки та конфіденційності.

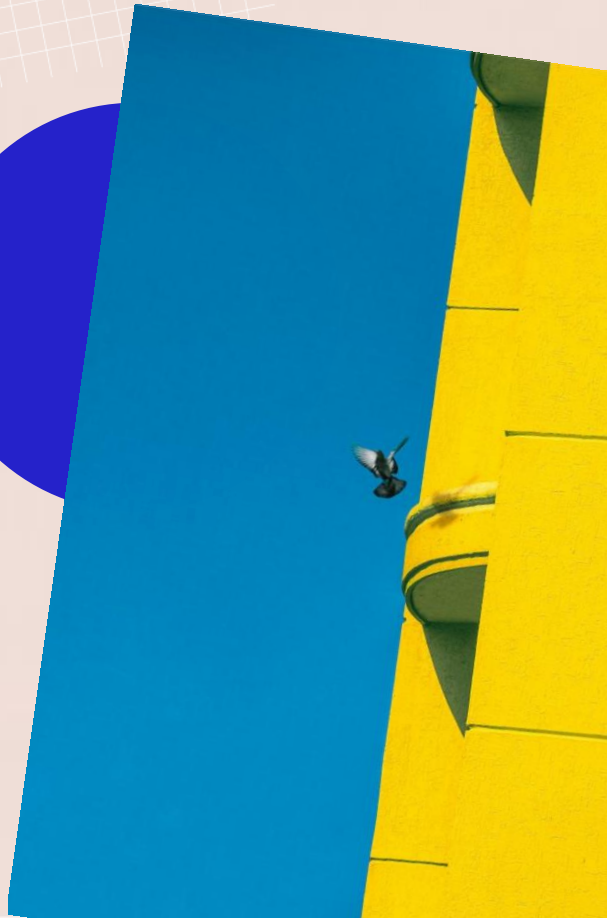
1. Обмеження обробки особливих категорій даних: GDPR забороняє обробку особливих категорій даних, таких як релігійні, расові, медичні дані тощо, без вираженої згоди суб'єкта даних або законної підстави.

1. Міжнародний обсяг: GDPR має міжнародний обсяг. Це означає, що будь-яка організація, яка обробляє дані громадян ЄС, повинна дотримуватися цих правил, навіть якщо вона розташована за межами ЄС.

GDPR впливає на рекламні технології та диджитал рекламу, оскільки вони широко використовують особисті дані користувачів для спрямування реклами. Регламент обмежує збір та використання даних без згоди користувачів, а також вимагає, щоб компанії були прозорі у відношенні до того, як вони обробляють дані. Утримання і розгортання інфраструктури для обробки даних також відіграють суттєву роль в розвитку технологічного стану українського рекламного та маркетингового ринку.

iab ukraine

ЧОМУ GDPR ВАЖЛИВИЙ ДЛЯ УКРАЇНИ



Чому GDPR важливий для України

Олександра Булигіна
Керівник комітету Programmatic IAB Україна, Директор, Amnet, member of Dentsu Aegis Network Ukraine

У сучасному цифровому світі обробка особистих даних стала невід'ємною частиною багатьох аспектів життя, включаючи бізнес та торгівлю. Загальний регламент про захист даних, відомий як GDPR, є однією з ключових ініціатив, які створюють рамки для захисту особистих даних громадян.

У цьому розділі ми розглянемо для чого саме GDPR є настільки важливим в Україні. Ми розглянемо ключові аспекти цієї ініціативи та визначимо, як вона впливає на українські компанії, громадян та бізнесове середовище загалом. Розглядаючи важливість GDPR в контексті України, ми зрозуміємо, чому впровадження цього Регламенту є необхідним та як воно може вплинути на розвиток сучасного суспільства та бізнесу в Україні.

Що дає дотримання GDPR в Україні

1. Робота з міжнародними партнерами: Українські компанії часто співпрацюють з європейськими партнерами і клієнтами. Якщо ваша компанія обробляє особисті дані європейських громадян, то дотримання GDPR стає обов'язковим. Це важливо для збереження партнерських відносин та доступу до міжнародних ринків.

2. Захист особистих даних громадян і негромадян: GDPR забезпечує високий рівень захисту особистих даних громадян. В Україні це особливо важливо, оскільки ми, як ринок, маємо бути впевненими що не тільки дані громадян України, а й дані громадян ЄС повинні залишатись конфіденційними та безпечними від несанкціонованого доступу та витоку, що зумовлено екстериторіальним характером GDPR.

3. Забезпечення довіри клієнтів: споживачі стають все більше обізнаними щодо правил обробки їхніх особистих даних. Дотримання GDPR підвищує довіру споживачів до бренду та послуг компанії клієнтів та агенцій в ринку та відкриває можливості до прозорої роботи з вендорами.

4. Уникнення штрафів та правових проблем: GDPR передбачає значні штрафи за порушення правил обробки особистих даних. Впровадження цих правил в Україні допомагає уникнути високих штрафів та можливих правових проблем, які можуть виникнути внаслідок порушення законодавства.

5. Підготовка до майбутнього: Цифрова трансформація в Україні продовжується, і обробка особистих даних стає все важливішою складовою сучасного бізнесу. Впровадження GDPR допомагає компаніям підготуватися до майбутніх викликів у сфері захисту даних та створює фундамент для інновацій та росту, а також швидкого розгортання стандартів в момент впровадження GDPR в Україні.

Отже, GDPR в Україні необхідний для забезпечення міжнародної співпраці, захисту особистих даних громадян, підвищення довіри споживачів, уникнення правових ризиків та підготовки до цифрового майбутнього. Впровадження цих стандартів є важливим кроком для українських компаній та організацій, які прагнуть успішно функціонувати в сучасному світі.

Для чого GDPR потрібен в Україні

Ігор Зайчук
Комерційний директор MEGOGO

Загальний регламент захисту даних (General Data Protection Regulation, далі — GDPR) — це документ, який визначає стандарти та вимоги до отримання, обробки та роботи з персональними даними користувачів з Європейського Союзу. GDPR прагне посилити захист конфіденційності європейських громадян, переконавшись, що люди та компанії, які обробляють персональні дані європейських громадян, роблять це належним і безпечним способом. Незважаючи на те, що GDPR є внутрішнім актом ЄС, у певних випадках він має екстериторіальну дію. Наприклад, коли українська компанія орієнтується на користувачів з ЄС, вона має обов'язок бути GDPR compliance.

На сьогодні, багато українських компаній, надаючи послуги користувачам з ЄС, відповідають вимогам GDPR, але таких компаній мізер у відношенні до всього українського бізнесу.

Водночас відповідність українського бізнесу вимогам GDPR compliance має ряд переваг, які потенційно можуть відкрити для компаній нові точки росту.

Переваги запровадження вимог GDPR в Україні

1. Масштабування бізнесу;
Так, компанії, які відповідатимуть вимогам GDPR, матимуть змогу працювати на європейський ринок. Така можливість стане доступна як видавцям так і клієнтам/агенціям.

2. Збільшення довіри до компаній з України;
Компанія зі статусом GDPR compliance має певний кредит довіри, щодо себе та своєї роботи, зокрема з персональними даними користувачів. Тим самим, користувачі контенту та європейський бізнес будуть охочіше працювати з компаніями, які виконують вимоги GDPR.

3. GDPR compliance – це конкурентна перевага;
Будь-якому бізнесу потрібно бути конкурентоспроможним на ринку та мати конкурентні переваги, які забезпечать стабільне функціонування та ріст. GDPR compliance компанії – це перевага, яка формує ділову репутації компанії як такої, що цінує персональні дані своїх клієнтів. Більше того, перевага GDPR compliance може стати вирішальною при виборі кінцевим користувачем чи іншим бізнесом, компанії чиїми клієнтами вони стануть.

4. Перебування в контексті тенденцій демократичних країн;
Не буде перебільшенням сказати, що захист персональних даних користувачів – це один з ключових напрямів роботи демократичних країнах. Тому, робота в напрямку відповідності вимогам GDPR, дозволить українському бізнесу бути частиною великої спільноти та наблизитися до розуміння особливостей роботи та практики застосування правил роботи з персональними даними в європейських країнах.

Що дає дотримання GDPR видавцям

Андрій Боборикін
Керівник комітету Publisher
Виконавчий директор суспільно-політичного інтернет-ЗМІ «Українська правда»

Може здатися, що цей гайд стосується насамперед брендів, рекламних агентств і компаній, що працюють в adtech, але в контексті медіабізнесу дотримання GDPR - це не просто один зі сценаріїв, а екзистенційна необхідність.

В українських медіа поки що лише зароджується культура управління персональними даними, тому для наших видань усі ці попапи і тумблери з різними видами доступу, які ми час від часу бачимо на західних сайтах, здаються перебором, який псує користувацький досвід. До того ж небагато українських медіа насправді хоч щось роблять із даними своїх читачів. Хай там як, від цих глобальних процесів українським паблішерам уже, на жаль, не втекти, і краще почати розбиратися в цьому якомога раніше.

Вимушений переїзд мільйонів українців за кордон для більшості вітчизняних медіа, включно з великими національними виданнями на кшталт "Української правди", а також невеликими регіональними сайтами, означає, що значна частина цільової аудиторії за півтора роки трансформувалася з української в зарубіжну. Тобто, навіть якщо ви нічого не змінювали у своїй редакційній стратегії, ваше видання вже автоматично стало значно сильніше інтегроване в західноєвропейський медіаринок, де діють свої вимоги до політик використання користувацьких даних. Через це головна і найбільша перевага впровадження стандартів GDPR на сайті вашого видання полягає в тому, що ви зможете ефективно монетизувати ту частину вашої аудиторії, яка знаходиться в країнах ЄС.

Що надає дотримання GDPR видавцям

Є й інші переваги. Як я вже написав вище, небагато українських медіа активно використовують можливості роботи з користувацькими даними у себе на сайті, хоча, починаючи з відключення підтримки third-party cookies наступного року стратегія роботи з даними стане важливою складовою стратегії монетизації будь-якого комерційного видання. Відповідно впровадження політик GDPR може стати певним “тренуванням” як продуктової команди, так і частини аудиторії. Зрештою є необхідність привчати й українську аудиторію до цих стандартів, адже прихід GDPR в Україну неминучий.

Те, що ще донедавна здавалося забаганкою європейських регуляторів, уже зараз на наших очах стає частиною довгострокових стратегій усіх учасників цифрового ринку. Вже можна з упевненістю сказати, що майбутнє монетизації медіапроєктів у будь-якій точці світу істотно залежить від правильної роботи з даними користувачів. Відповідні інвестиції в експертизу команди та продуктові рішення в цій галузі через кілька років визначатимуть маржинальність усього медіабізнесу. Подумати про свою GDPR-first стратегію кожен медіаменеджер повинен уже сьогодні.

iab ukraine

ВПЛИВ GDPR НА ЄВРОПУ І ЯКІ ЗМІНИ МОЖУТЬ БУТИ В УКРАЇНІ

Що приніс GDPR для Європи?

Олександра Булигіна
Керівник комітету Programmatic IAB Україна, Директор, Amnet, member of Dentsu Aegis Network Ukraine

Після введення Загального регламенту про захист даних (GDPR) в Європі стало ясно, що цей закон спричинив значні зміни в підходах до обробки особистих даних.

Один із прикладів - право громадян ЄС на "право бути забутим", що означає право вимагати видалення своїх особистих даних з систем компаній та їх маркетингових та рекламних активностей.
Для прикладу, якщо користувач залишає коментар на веб-сайті або магазині в Інтернеті та потім бажає видалити свій акаунт, компанія зобов'язана не лише видалити всі його особисті дані, але і припинити обробку цих даних третіми сторонами. Це сприяє більшому контролю громадян над їхніми даними. Та в рамках маркетингу і реклами значно сповільнює і ускладнює розвиток персональної комунікації з клієнтом.
GDPR став значущим кроком у сфері захисту особистих даних в Європейському Союзі. Розгляньмо, які впливи GDPR спричинив у Європі та які можливі наслідки він може мати для України.

Вплив GDPR на Європу:

- Підвищення рівня захисту особистих даних: Наприклад, громадяни тепер мають право контролювати та переносити свої дані між різними сервісами, а також припиняти взаємодію з сервісами і видаляти повністю свої дані через них. Так з провадженням GDPR значно скоротився об‘єм e-mail розсилок, через необхідність підтвердження підписки користувачем, проте з іншого боку цей кейс про більш якісну комунікацію зі споживачем та більшу увагу саме до брендів.

- Зміцнення прав споживачів: Цей Регламент розширив права споживачів на отримання інформації про обробку їхніх даних. Споживачі мають право звертатися до організацій з запитами про доступ до своїх даних.

Можливі наслідки для України

- Введення суворих штрафів за порушення: Це стимулює організації дотримуватися правил обробки даних та забезпечувати їх безпеку.

- Поліпшення захисту особистих даних: Впровадження GDPR-подібних стандартів в Україні може покращити рівень захисту особистих даних громадян. Наприклад, банки та медичні установи зобов'язані будуть зберігати дані безпечно та конфіденційно і взаємодіяти більш виважено для того, щоб не втратити споживача.

- Збільшення інтересу іноземних інвесторів: Впровадження стандартів GDPR може зробити Україну більш привабливою для іноземних інвесторів, оскільки це свідчить про високий рівень захисту даних і зрозумілу інфраструктуру їх обробки, що зменшує шанси на штрафи.

- Підвищення довіри споживачів: Впровадження GDPR сприяє підвищенню довіри споживачів до українських компаній та послуг, що обробляють їхні дані. Цей тренд наразі можна спостерігати в розвинених ринках у найбільш молодших поколінь споживачів, що звертають активну увагу на «екологічність» брендів в різних сферах, в тому числі й про використання й відношення до даних про споживача.

- Зосередженість на кібербезпеці: Організації будуть більше уваги приділяти кібербезпеці, оскільки GDPR покладає великий акцент на безпеку даних та вимагає звітності про порушення даних. Відтак наш сильний IT сектор може ще більш зміцніти і бути драйвером рішень для ринків маркетингу й реклами, як і в інших секторах.

Відтак, впровадження стандартів GDPR в Україні має потенціал стати кроком до покращення якості захисту особистих даних громадян, підвищення довіри до українських компаній та привабливості для іноземних інвесторів. Важливо розуміти, що захист особистих даних - це не лише вимога, але і можливість для України визначити себе як сучасну та відповідальну країну в цифровому віці.

Для чого GDPR потрібен в Україні?

Ігор Зайчук
Комерційний директор MEGOGO

Хоча, GDPR - це документ ЄС, і він має діяти в європейських країнах, останні кілька років існування Регламенту показали, що правила GDPR вплинули на весь світ. За 5 років дії GDPR, простежуються певні загальні наслідки від впровадження GDPR. В тому числі це стосується і України, хоча для українського бізнесу такі наслідки простежуються рідше і в менших обсягах.

Отже, які наслідки GDPR?

1. Збільшення влади та контролю користувачів над своїми даними, які вони передають на обробку.
З запровадженням GDPR користувачі отримали вибір щодо даних, які вони хочуть передавати на обробку, та цілей, з якими їх дані будуть оброблятися. Водночас користувачі не завжди хочуть цією владою скористатися, даючи згоду на обробку своїх даних у максимальному з можливих обсязів.

2. Дані користувачів стали надзвичайно цінними.
Надання персоналізованих пропозицій прямо залежить від обсягів наданих користувачами даних та згоди на їх обробку. Таким чином, в обмін на детальну інформацію про себе користувач може отримати гіперперсоналізовану взаємодію з бізнесом.

3. Компанії проробили колосальну роботу по впровадженню стандартів та виконаню вимог GDPR.
GDPR compliance потребував залучення багатьох спеціалістів та витрачання додаткових ресурсів (час, гроші, кадри). Не дивлячись на вже проороблену роботу, відповідність вимогам GDPR є надзвичайно динамічним процесом, тому компаніям доведеться витрачати ще більше ресурсів для забезпеченню приватності та виконання вимог GDPR в майбутньому.

Для чого GDPR потрібен в Україні?

4. Маленький бізнес постраждав.
Маленький бізнес, який фінансово нездатний найняти відповідних спеціалістів, чи платити профільним компаніям за забезпечення відповідності GDPR, зазнали значних труднощів у впровадженні GDPR. У більш далекій перспективі це призведе до того, що малий бізнес втратить здатність конкурувати з більшими компаніями, які мають достатню фінансову спроможність для виконання вимог GDPR.

5. Вивчення, застосування та виконання вимог GDPR – це новий бізнес.
Допомога у виконанні вимог GDPR - є затребуваний вид послуг, бізнес з надання яких заробляє все більше і більше грошей. В тому числі з'являються технологічні платформи та рішення, які розв'язують ряд проблем з впровадженням приватності, що певною мірою спрощує процес проходження GDPR compliance. З іншого боку це призводить до подорожчання таких послуг та зменшення їх доступності.

6. Необхідність у додатковому регулюванні та кваліфікованих спеціалістах.
Правозастосування та виконання вимог GDPR потребує роботи контролюючих та регулюючих органів. Так, в кожній країні ЄС створюються та діють наглядові органи, які слідкують за виконанням GDPR, надають роз'яснення та рекомендації для ефективнішого правозастосування.

Не менш важливим є наявність кваліфікованих кадрів, які зможуть роботи бізнес GDPR compliance. Наразі розробляються та запроваджуються різноманітні освітні курси та загальні підходи для оцінки кваліфікації спеціалістів у галузі приватності.

ЩО ТАКЕ ПЕРСОНАЛЬНІ ДАНІ ТА ЇХ РІЗНОВИДИ

Персональні дані та їх різновиди

Дар’я Маліхатко
Data Science Director в Publicis Groupe, керівниця комітету Data

В попередніх розділах, висвітлюючи суть, мету та важливість GDPR та його інтеграції в роботу компаній в Україні, ми неодноразово посилались на те, що GDPR був прийнятий з метою захисту особистих (або персональних) даних громадян. Фактично GDPR встановлює ряд ключових принципів та обов'язків для підприємств щодо роботи з персональними даними.
Однак, важливим питанням залишається визначення: що ж є персональними даними згідно з Загальним регламентом про захист даних. Визначення персональних даних відповідно до GDPR є дуже широким і навмисно всеохопним.

Персональні дані відповідно до GDPR – будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи 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

GDPR також визначає **спеціальні категорії чутливих персональних даних**:

- дані, що розкривають расову чи етнічну приналежність,
- політичні переконання
- релігійні чи філософські вірування
- членство в професійних спілках
- 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

Персональні дані та їх різновиди

GDPR вводить концепцію **псевдонімізованих даних** як підмножини **персональних даних**, які не можна віднести до конкретного суб'єкта даних без додаткової інформації.

Псевдонімізація - це обробка персональних даних у такий спосіб, що персональні дані більше не можна віднести до конкретного суб'єкта даних без використання додаткової інформації.

Така обробка може виключати дані з певних зобов'язань GDPR, а саме:

- доступ суб'єкта
- право на виправлення, видалення та перенесення даних

Псевдонімізація визнається запобіжником, який

1. Зменшує ризики для суб'єктів даних
2. Допомагає компаніям виконувати свої зобов'язання щодо захисту даних
3. Сприяє допустимій обробці для вторинного використання

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 може, використовуватися для дослідницьких цілей у безпечний для конфіденційності спосіб.

Анонімізація — це «метод, що застосовується до персональних даних з метою досягнення незворотної деідентифікації. Якщо компанія зберігає дані, які є дійсно анонімними, GDPR не застосовується до цих даних.

НАПРИКЛАД:

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.

Чи є Персональними даними Онлайн-ідентифікатори?

Сфера цифрової реклами та інші бізнеси, 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.

Однак, важливо розуміти, що ці онлайн-ідентифікатори, все ж підпадають під сферу персональних даних відповідно до GDPR. Згідно з GDPR фізичні особи можуть бути пов’язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, додатків, інструментів чи протоколів. Це може залишити підказки, які **можна використати для створення профілів фізичних осіб та їхньої ідентифікації.**

Тому, онлайн-ідентифікатори, повинні розглядатися саме як **персональні дані**, якщо не може бути наведено обґрунтований аргумент про те, що суб'єкт даних не може бути ідентифікованим і не може бути виокремленим.

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.

НАПРИКЛАД:

IP-адреса є прикладом даних, які можуть бути анонімними даними, псевдонімізованими персональними даними або неанонімними персональними даними, залежно від конкретних обставин.

Дані, які не є персональними даними, виходять за рамки застосування GDPR.

ЩО ТАКЕ CMPs І ДЛЯ ЧОГО ВОНИ ПОТРІБНІ

Що таке CMPs і для чого вони потрібні

Олексій Підлісняк
Head of Media Buying and implementation, Admixer Advertising

CMP (Consent Management Platform) - це платформа управління згодами, яка використовується для збору, зберігання та управління згодами користувачів на обробку їхніх особистих даних. CMP є важливою частиною забезпечення відповідності з законами про захист особистих даних, такими як Регламент про загальний захист даних (GDPR) в Європейському Союзі та іншими аналогічними законами в інших регіонах.

Основні функції CMP включають в себе:

- Збір згоди: CMP надає користувачам можливість надавати свою згоду або відмовлятися від неї на обробку їхніх особистих даних, таких як файли cookie, IP-адреси, ідентифікатори пристроїв та інші дані, які збираються під час відвідування веб-сайтів;

- Контроль над налаштуваннями приватності: Користувачі можуть налаштовувати рівень конфіденційності та вибирати які типи даних вони готові надавати або не надавати, а також налаштовувати персоналізовані налаштування приватності;

- Документація та зберігання: CMP забезпечує документацію та зберігання згоди користувачів, що дозволяє організаціям доводити їхню відповідність законодавству про захист даних;

- Моніторинг та звітність: CMP може надавати звіти та аналітику щодо використання згоди користувачами, а також слідкувати за відповідністю політикам приватності та вимогам законодавства.

Що таке CMPs і для чого вони потрібні

GDPR включає декілька статей та пунктів, які стосуються згоди та обробки особистих даних. Деякі з них:

- Стаття 7 (Згода): GDPR регулює, що згода користувача має бути вільно даною, специфічною, інформованою та виразною.

- Стаття 12 (Зрозумілість і доступність інформації): Вимагається, щоб інформація про обробку особистих даних була доступною, зрозумілою та легкою для користувачів. CMP системи допомагають виконати цю вимогу.

- Стаття 21 (Право на відмову від обробки): Користувачі мають право відмовитися від обробки їхніх особистих даних. CMP системи дозволяють користувачам здійснювати це право.

Використання CMP може допомогти виконувати вимоги GDPR, забезпечуючи зручний і прозорий спосіб отримання та відмови для згоди від користувачів щодо обробки їхніх особистих даних. Таким чином, хоча GDPR не зазначає обов'язкового використання CMP, воно може бути важливим інструментом для досягнення відповідності з цим регуляторним актом. Багато мереж вже вимагають наявність CMP на ресурсі.

Погоджені CMP IAB EU: https://iabeurope.eu/cmp-list/

Що таке TCF і для чого він потрібен

Юрій Горохов
Заступник керівника комітету Programmatic IAB Україна, CTO Adtelligent Inc

TCF - це уніфікований набір стандартів та підходів для дотримання вимог GDPR та ePrivacy directive.

Особливо треба підкреслити:

TC string - це нормований формат передачі консенту(дозволу) користувача на обробку персональних даних для программатик екосистеми

Global Vendor List (GVL) - це глобальній лист (приблизно з 1000 компаній дотичних до реклами, чи аналітки або даних) з обґрунтуванням цілей та засобів обробки даних.

Серед інших розуміння цих двох механізмів є найважливішим для загального розуміння функціонування програматік сьогодні.

Розуміючи, що істотна частина відповідальності за дотримання норм обробки даних ланцюжком программатик покладено саме на видавця, а крім розуміння базових принципів треба пильнувати за окремими поясненнями від єврокомісії та слідкувати за оновленням версії протоколів(як наприклад TCF 2.2) - мабуть програмна імплементація для кожного окремого видавця не є найліпшим вибором. Є окремий клас платформ як Consent Managment Platfroms(CMP), котрі беруть на себе значну частину цієї задачі. Включно з проходження сертифікації у TCF як платформи для управління згодою користувача, але не виключно, ці платформи істотно покращують життя видавців. Беручи на себе не тільки задачі программатик екосистеми, але і допомагають регулювати власні куки видавця, та окремі системи, як то чат-боти чи CRM та інші.

Отже, TCF і CMP допомагають оптимізувати трафік і покращити продуктивність мережі, кожен з них вирішує свої завдання в цьому контексті.

iab ukraine

POV ЮРИСТІВ

POV юриста

Олена Андрієнко

Заступник директора з правових питань Publicis Groupe Ukraine
Членкиня Наглядової ради Всеукраїнської Рекламної Коаліції

1. Впровадження GDPR в Україні - питання часу, причому найближчого
Відповідно до ст. 15 Угоди про асоціацію України та ЄС "Сторони домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи". Тому з осені 2022 року у Парламенті очікує розгляду відповідний законопроєкт.

2. Відповідність GPDR - конкурентна перевага при виході на ринок ЄС
Йдеться про перевірку не лише клієнтами з ЄС та міжнародними клієнтами в Україні, але й великими міжнародними підрядниками потенційних контрагентів з України на відповідність GDPR. Невідповідність умовам GDPR може стати причиною відмови від співпраці.

3. Війна лише прискорює перехід до GDPR
Якщо хтось із ваших працівників, перебуваючи в ЄС, працює у вашій компанії, ваша компанія повинна відповідати вимогам GDPR вже сьогодні, адже ви неминуче обробляєте персональні дані такого працівника чи працівниці.
Якщо ваша компанія таргетує рекламу на українців, яка наразі перебувають в ЄС, ви також повинні відповідати вимогам GDPR. Ймовірність, що серед вашої аудиторії є наші співвітчизники в ЄС надзвичайно висока, адже наразі кількість українських біженців у ЄС за даними ООН наближається до 6 млн. Це кожний 7-ий українець чи українка із тих, що до повномасштабного вторгнення жили в Україні.

4. Впровадження GPDR безперечно вимагає ресурсів, проте воно необхідне - як щеплення від штрафів
З огляду на п. 3, ризики зазнати санкцій через невиконання вимог GDPR наразі існують у багатьох українських компаній. Тож планове запровадження відповідних процедур - життєво важливе, адже зекономлені кошти - це зароблені кошти. Моя колега поділиться корисним досвідом, як таке запровадження відбувається на практиці.

POV юриста

Ольга Антонюк
LL.M., CIPP/E, CIPP/US
Голова Юридичного департаменту / DPO в Adtelligent Inc

Обсяг змін, яких вимагає GDPR від бізнесів, дотичних до персональних даних користувачів, на перший погляд вражає. І це цілком природно, адже впровадження всіх необхідних практик, політик і контролів у бізнес процеси на потоці наводить на аналогію з хірургічною операцією на працюючому серці. Однак, не варто давати волю сумнівам чи залишатись осторонь, керуючись виключно міркуваннями складнощів запровадження GDPR, адже виважений і послідовний підхід до цього процесу здатний мінімізувати можливі незручності та сприяти м'якій та поступовій трансформації відповідних корпоративних практик без шкоди для ключових бізнес процесів. В даному гайді перелічено основні кроки, необхідні для дотримання вимог GDPR, однак, з власного досвіду ми усвідомлюємо, що способи і порядок їх практичного впровадження можуть здаватися неочевидними для тих, хто стикається з цим вперше.

На практиці найбільш доцільним в першу чергу є призначення відповідальної особи, яка адмініструватиме весь процес переходу, забезпечуватиме відповідні комунікації між окремими підрозділами компанії і надалі стане уповноваженим з приватності даних. Саме цей співробітник у співпраці з розробниками та менеджерами проєктів зможе послідовно провести аудит даних, маппінг даних та відслідковування точок трансферів даних – моментів отримання персональних даних внутрішніми системами компанії та передачі їх назовні третім особам, визначити сутність, способи та мету обробки таких даних. Після цього можна буде побачити цілісну картину циклу життя персональних даних, якими оперує бізнес, і належним чином оцінити як необхідні безпекові заходи, так і невідповідності в процесах обробки, зберігання або передачі щодо вимог GDPR.

POV юриста

Виходячи з результатів такої оцінки, уповноважений з приватності даних має розробити індивідуальний план заходів по усуненню виявлених відхилень та недоліків. Варто зауважити, що впровадження такого плану може бути досить тривалим процесом, але частину заходів можна проводити паралельно та одночасно. Наприклад, створення документального підґрунтя для обробки та передачі персональних даних – журналу обліку обробки персональних даних, угод про обробку персональних даних, політик приватності тощо – може розпочинатись одночасно з впровадженням безпекових заходів, базовим навчанням персоналу, впровадженням практик аудитів даних підрядників та іншими подібними кроками.

Досвід впровадження GDPR у працюючих бізнесах показує, що, хоча базової відповідності вимогам можна досягти у 3-6 місячні терміни (залежно від розмірів бізнесу та обсягів обробки даних, яка ним виконується на щоденній основі), проведення всіх необхідних заходів і підтримка відповідності у довгостроковій перспективі, включаючи можливі оцінки впливу обробки персональних даних та впорядкування обробки запитів від суб'єктів даних, може потребувати значно більше часу. Тим не менш, проведена один раз, ця робота створить надійну основу для подальшої полегшеної адаптації та стійкості бізнесу до нових викликів, які виникають у царині захисту приватності персональних даних і загальної інформаційної безпеки на регулярній основі.

iab ukraine

СЛОВНИК ТЕРМІНІВ

Словник термінів

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 місцезнаходження, 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.

Словник термінів

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.

Словник термінів

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).

Словник термінів

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)

iab ukraine

ОСНОВНІ РЕКОМЕНДАЦІЇ ДЛЯ ДОТРИМАННЯ ВИМОГ GDPR

Основні рекомендації для дотримання вимог GDPR

Підзвітність та облік є центральною темою GDPR, всі операції з даними, їх мета та заходи безпеки, що застосовуються, мають документуватися належним чином. Нижче наведені основні рекомендації, якими можуть скористатись компанії для дотримання вимог GDPR.

Крок 1 - Визначення мети та способу обробки даних
На початку процесу документування необхідно визначити мету та способи обробки даних, провести дата маппінг з особливою увагою до тих груп даних, які за GDPR віднесені до категорії чутливих.

Крок 2 - Залучення всіх департаментів компанії
До процесів обліку та документування мають бути залучені всі департаменти компанії, адже завдання по дотриманню вимог щодо обробки персональних даних тим чи іншим чином стосуються кожного співробітника компанії.

Крок 3 - Детальний розгляд усіх процесів в компанії
При документуванні процедур з обробки даних потрібно розглянути всі процеси в компанії, відповідаючи на питання «що», «де», «коли», «чому», а також враховувати очікувані наслідки для кожного процесу та провести аналіз ризиків. Це стосується всіх аспектів діяльності – клієнти, підрядники, працівники та кандидати, штатні та позаштатні.

Для документування враховуються джерело даних, мета і зміст їх обробки, строки їх зберігання у внутрішніх системах компанії, спосіб видалення та архівації, технології та механізми забезпечення внутрішньої безпеки та захисту від зовнішнього втручання, а також адресати, мета та підстави для передачі третім особам.

Крок 4 - Проведення аудиту даних
Перед або під час документування важливо провести аудит даних, під час якого звертати увагу на дотримання ключових принципів GDPR: прозорості, законності та добросовісності обробки, мінімізації даних, точності документування. Під час аудиту також проводиться оцінка ризиків, які має або може мати ваша обробка, для законних інтересів суб'єктів персональних даних.

Крок 5 - Виправлення невідповідностей вимогам GDPR
Всі невідповідності, неточності або можливі порушення вимог GDPR, виявлені під час аудиту даних мають бути виправлені, процеси обробки належно скориговані, а безпекові процедури приведені у відповідність. Для цього створюється покроковий план, розроблений відповідно до потреб компанії, виявлених під час аудиту даних.

Основні рекомендації для дотримання вимог GDPR

Крок 6 - Проведення аналізу впливу на захищеність даних
У випадку виявлення під час аудиту даних фактів новаторського способу обробки даних, обробки значних масивів персональних даних або обробки, що включає автоматизоване прийняття юридично значущих рішень щодо суб'єктів персональних даних або їх профілювання, необхідно також провести аналіз впливу на захищеність даних та оцінити можливі додаткові ризики та способи їх мінімізації.

Крок 7 - Навчання персоналу
Додаткової уваги потребують процеси запровадження регулярного тренування персоналу з питань захисту персональних даних та створення плану реагування на безпекові виклики та інциденти. Персонал компанії має бути поінформованим не лише про порядок дій у випадку зламу, витоку, крадіжки персональних даних, якими оперує компанія, але і про профілактичні заходи щодо безпеки даних.

Крок 8 - Робота з партнерами та підрядниками
Не менш важливо приділяти увагу питанням відповідності вимогам GDPR і при виборі партнерів та підрядників, з якими здійснюється обмін персональними даними суб'єктів. Всі такі передачі мають бути належним чином обґрунтовані, документально оформлені, а самі такі партнери та підрядники також мають дотримуватися вимог GDPR під час обробки персональних даних. Цій меті служать угоди про обробку персональних даних, які мають укладатися між компаніями, задіяними в інфраструктурі передачі даних.

Крок 9 - Призначення уповноваженого з приватності даних
GDPR також вимагає призначити уповноваженого з приватності даних (штатного співробітника або зовнішнього підрядника) та офіційного представника у ЄС (для компаній, що не мають зареєстрованого офісу чи представництва у жодній з країн ЄС). Окрім формального виконання вимог GDPR ці призначення також сприятимуть спрощенню процесів виконання решти зобов'язань, покладених GDPR на компанії.

Крок 10 - Внесення змін до політик приватності
Всі вищезазначені процедури та призначення можуть потребувати подальшого внесення змін до політик приватності компанії, як внутрішніх (що регулюють дії працівників та управлінців), так і зовнішніх (що викладені на сайті компанії та забезпечують належне інформування суб'єктів персональних даних). Ці зміни мають бути внесені, а відповідні політики мають перевірятись та оновлюватись на регулярній основі для забезпечення повного дотримання прав суб'єктів персональних даних.

Корисна інформація

- Посилання на повний Гайд “ЗНАЙОМСТВО З GDPR”
- Посилання на етер “Знайомство з GDPR”
- Із загальним Регламентом захисту даних GDPR можна ознайомитися тут

Команда

Олександра Булигіна
Керівник комітету Programmatic IAB Україна,
Директор, Amnet, member of
Dentsu Aegis Network Ukraine

Ігор Зайчук
Комерційний директор MEGOGO

Дар'я Маліхатко
Data Science Director в Publicis Groupe, керівниця комітету Data

Олена Андрієнко
Заступник директора з правових питань
Publicis Groupe Ukraine
Членкиня Наглядової ради Всеукраїнської Рекламної Коаліці

Ольга Антонюк
LL.M., CIPP/E, CIPP/US
Голова Юридичного департаменту / DPO в Adtelligent Inc

Команда

Олексій Підлісняк
Head of Media Buying and implementation, Admixer Advertising

Юрій Горохов
Заступник керівника комітету Programmatic IAB Україна, CTO Adtelligent Inc

Андрій Боборикін
Керівник комітету Publisher
Виконавчий директор суспільно-політичного інтернет-ЗМІ «Українська правда»

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