Настанови

Настанови 05/2020 щодо надання згоди відповідно до Регламенту 2016/679

Версія 1.1

Прийнято 4 травня 2020 року

Прийнято

Цей переклад не є офіційним перекладом Європейської ради із захисту даних. Переклад здійснено за фінансової підтримки GIZ у рамках Регіонального проєкту «Реформа державного управління в країнах Східного партнерства III» та тісній співпраці з Офісом Уповноваженого Верховної Ради України з прав людини та Європейською радою із захисту даних. Правильність перекладу підтверджено Офісом Уповноваженого Верховної Ради України з прав людини

Історія версій

Версія 1.1	13 травня 2020 року	Виправлення форматування
Версія 1.0	4 травня 2020 року	Затвердження Настанов

Прийнято

Зміст

Прийнято

Цей переклад не є офіційним перекладом Європейської ради із захисту даних. Переклад здійснено за фінансової підтримки GIZ у рамках Регіонального проєкту «Реформа державного управління в країнах Східного партнерства III» та тісній співпраці з Офісом Уповноваженого Верховної Ради України з прав людини та Європейською радою із захисту даних. Правильність перекладу підтверджено Офісом Уповноваженого Верховної Ради України з прав людини

ЄВРОПЕЙСЬКА РАДА ІЗ ЗАХИСТУ ДАНИХ

Беручи до уваги статтю 70(1)(e) Регламенту Європейського Парламенту та Ради 2016/679/ЄС від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (далі — «GDPR»).

Беручи до уваги Угоду про ЄЕП, зокрема, Додаток XI та Протокол 37 до неї, зі змінами, внесеними Рішенням Спільного Комітету ЄЕП № 154/2018 від 6 липня 2018 року[1],

Беручи до уваги статтю 12 та статтю 22 його Регламенту,

Беручи до уваги Настанови Робочої групи за статтею 29 щодо надання згоди відповідно до Регламенту 2016/679, РД 259 версія 01,

ПРИЙНЯЛА ТАКІ НАСТАНОВИ

0 ПЕРЕДМОВА

10 квітня 2018 року Робоча група за статтею 29 ухвалила Настанови щодо надання згоди відповідно до Регламенту 2016/679 (РД 259, версія 01), які були схвалені Європейською радою із захисту даних (далі — «EDPB») на її першому пленарному засіданні. Цей документ є дещо оновленою версією цих Настанов. Будь-яке посилання на Настанови Робочої групи за статтею 29 щодо надання згоди (РД 259, версія 01) відтепер слід тлумачити як посилання на ці настанови.

EDPB зауважила, що існує потреба в подальших роз'ясненнях, зокрема, щодо двох питань:

1 Дійсність згоди, наданої суб'єктом даних при взаємодії з так званими «бар'єрами файлів cookie»;
2 Приклад 16 про прокручування та надання згоди.

Пункти, що стосуються цих двох питань, були переглянуті та оновлені, в той час, як решта документа була залишена без змін, за винятком редакційних правок. Зміни стосуються, зокрема, такого:

- Розділ про обумовленість (пункти 38-41).
- Розділ про однозначне зазначення побажань (пункт 86)

[1] Посилання на «держави-члени», що містяться в цьому документі, слід розуміти як посилання на «держави-члени ЄЕП».

Прийнято

1 ВСТУП

1. Ці Настанови містять ретельний аналіз поняття згоди в Регламенті 2016/679, Загальному регламенті про захист даних (далі — «GDPR»). Поняття згоди, яке використовується в Директиві про захист даних (далі — Директива 95/46/ЄС) та в Директиві про приватність та електронні комунікації, наразі еволюціонувало. GDPR надає подальші роз'яснення та конкретизує вимоги щодо отримання та доведення дійсної згоди. Ці Настанови зосереджують увагу на цих змінах, надаючи практичні рекомендації щодо забезпечення відповідності GDPR та спираючись на Висновок 15/2011 Робочої групи за статтею 29 щодо надання згоди. Контролери зобов'язані впроваджувати інновації для пошуку нових рішень, які діють у рамках закону та краще підтримують захист персональних даних та інтересів суб'єктів даних.

2. Згода залишається однією із шести законних підстав для обробки персональних даних, перелічених у статті 6 GDPR.[2] Ініціюючи діяльність, яка передбачає обробку персональних даних, контролер завжди повинен витратити час на розгляд того, що буде належною законною підставою для передбачуваної обробки.

3. Як правило, згода може бути належною законною підставою лише в тому випадку, якщо суб'єкту даних пропонується контроль і реальний вибір щодо прийняття або відхилення запропонованих умов або відмови від них без шкоди для нього. Запитуючи згоду, контролер зобов'язаний оцінити, чи буде він відповідати всім вимогам для отримання дійсної згоди. Якщо згода отримана у повній відповідності до GDPR, вона є інструментом, який дає суб'єктам даних можливість контролювати, чи будуть оброблятися персональні дані, які їх стосуються. В іншому випадку контроль суб'єкта даних стає ілюзорним, а згода буде недійсною підставою для обробки, що робить діяльність з обробки незаконною.[3]

4. Існуючі Висновки Робочої групи за статтею 29 щодо надання згоди[4] залишаються актуальними, якщо вони відповідають новій нормативно-правовій базі, оскільки GDPR кодифікує існуючі настанови РД 29 та загальну належну практику, а більшість ключових елементів згоди залишаються незмінними відповідно до GDPR. Таким чином, у цьому документі EDPB розширює та доповнює попередні Висновки Робочої групи за статтею 29 на конкретні теми, які включають посилання на надання згоди відповідно до Директиви 95/46/ЄС, а не замінює їх.

---

[2] Стаття 9 GDPR містить перелік можливих винятків із заборони на обробку спеціальних категорій даних. Одним із таких винятків є ситуація, коли суб'єкт даних надає явну згоду на використання цих даних.

[3] Див. також Висновок 15/2011 Робочої групи за статтею 29 щодо визначення поняття згоди (РД 187), п. 6-8, та/або Висновок 06/2014 щодо поняття законних інтересів контролера даних відповідно до статті 7 Директиви 95/46/ЄС (РД 217), п. 9, 10, 13 і 14.

[4] Зокрема, Висновок 15/2011 щодо визначення поняття згоди (РД 187).

5. Як зазначила Робоча група за статтею 29 у своєму Висновку 15/2011 щодо визначення поняття згоди, запрошення осіб до надання згоди на операцію з обробки даних повинно відповідати суворим вимогам, оскільки це стосується основоположних прав суб'єктів даних, а контролер бажає здійснити операцію з обробки, яка була б незаконною без згоди суб'єкта даних.[5] Вирішальну роль надання згоди підкреслюють статті 7 і 8 Хартії основоположних прав Європейського Союзу. Крім того, отримання згоди також не скасовує і жодним чином не применшує зобов'язань контролера дотримуватися принципів обробки, закріплених у GDPR, особливо статті 5 GDPR щодо справедливості, необхідності та обґрунтованості, а також якості даних. Навіть якщо обробка персональних даних ґрунтується на згоді суб'єкта даних, це не легітимізує збір даних, який не є необхідним у зв'язку з визначеною метою обробки та є принципово несправедливим.[6]

6. Тим часом EDPB відомо про перегляд Директиви про приватність та електронні комунікації (2002/58/ЄС). Поняття згоди в проекті Регламенту про приватність та електронні комунікації залишається пов'язаним із поняттям згоди в GDPR.[7] Організації, ймовірно, потребуватимуть згоди відповідно до інструмента про приватність та електронні комунікації для більшості маркетингових повідомлень або маркетингових дзвінків в Інтернеті, а також для методів відстеження в Інтернеті, в тому числі за допомогою файлів cookie, додатків або іншого програмного забезпечення. EDPB вже надала рекомендації та вказівки європейським законодавцям стосовно Пропозиції щодо Регламенту про приватність та електронні комунікації.[8]

7. Що стосується існуючої Директиви про приватність та електронні комунікації, EDPB зазначає, що посилання на скасовану Директиву 95/46/ЄС повинні тлумачитися як посилання на GDPR.[9] Це також стосується посилань на надання згоди в чинній Директиві 2002/58/ЄС, оскільки Регламент про приватність та електронні комунікації (поки що) не набуде чинності з 25 травня 2018 року. Відповідно до статті 95 GDPR, додаткові зобов'язання щодо обробки у зв'язку з наданням загальнодоступних електронних комунікаційних послуг у мережах зв'язку загального користування не повинні накладатися, якщо Директива про приватність та електронні комунікації накладає конкретні зобов'язання з тією ж метою. EDPB зазначає, що вимоги щодо надання згоди відповідно до GDPR не вважаються «додатковим зобов'язанням», а скоріше передумовами для законної обробки. Таким чином, умови GDPR щодо отримання дійсної згоди застосовуються в ситуаціях, що підпадають під дію Директиви про приватність та електронні комунікації.

---

[5] Висновок 15/2011, сторінка про визначення поняття згоди (РД 187), с. 8.

[6] Див. також Висновок 15/2011 щодо визначення поняття згоди (РД 187) та статтю 5 GDPR.

[7] Згідно зі статтею 9 запропонованого Регламенту про приватність та електронні комунікації, застосовуються визначення та умови надання згоди, передбачені статтею 4(11) та статтею 7 GDPR.

[8] Див. заяву EDPB про приватність та електронні комунікації від 25.05.2018 р. та заяву EDPB 3/2019 про регулювання приватності та електронних комунікацій.

[9] Див. статтю 94 GDPR.

Прийнято

2 ЗГОДА В СТАТТІ 4(11) GDPR

8. Стаття 4(11) GDPR визначає згоду як *«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 обробку своїх персональних даних».*

9. Основне поняття згоди залишається аналогічним поняттю Директиви 95/46/ЄС, а згода є однією з законних підстав, на яких має ґрунтуватися обробка персональних даних, відповідно до статті 6 GDPR.[10] Окрім зміненого визначення в статті 4(11), GDPR надає додаткові вказівки в статті 7 та в преамбулах 32, 33, 42 та 43 щодо того, як контролер повинен діяти, щоб відповідати основним пунктам вимоги про надання згоди.

10. Зрештою, включення конкретних положень і пунктів про відкликання згоди підтверджує, що згода повинна бути оборотним рішенням і що залишається певний контроль з боку суб'єкта даних.

3 УМОВИ ДІЙСНОЇ ЗГОДИ

11. Стаття 4(11) GDPR передбачає, що 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 обробку своїх персональних даних.

12. У наступних розділах аналізується, якою мірою формулювання статті 4(11) вимагає від контролерів змінити свої запити/форми надання згоди, щоб забезпечити відповідність GDPR.[11]

---

[10] Згода визначена в Директиві 95/46/ЄС як *«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 обробку своїх персональних даних»*, яке має бути *«недвозначно надане»*, щоб зробити обробку персональних даних законною (стаття 7(a) Директиви 95/46/ЄС)). Див. Висновок 15/2011 Робочої групи за статтею 29 щодо визначення поняття згоди (РД 187) для прикладів щодо прийнятності згоди як законної підстави. У цьому Висновку Робоча група за статтею 29 надала вказівки щодо розмежування випадків, коли згода є належною законною підставою, від випадків, коли достатньо покладатися на законний інтерес (можливо, з можливістю відмовитися від участі), або коли рекомендується використовувати договірні відносини. Див. також Висновок 06/2014 Робочої групи за статтею 29, пункт III.1.2, с. 14 і далі. Явна згода також є одним із винятків із заборони на обробку спеціальних категорій даних: Див. статтю 9 GDPR.

[11] Для отримання вказівок щодо поточної діяльності з обробки даних на основі згоди в Директиві 95/46 див. главу 7 цього документа та статтю 171 GDPR.

Прийнято

3.1 Добровільно/вільно надана згода[12]

13. Пункт «вільно» передбачає реальний вибір і контроль для суб'єктів даних. Як правило, GDPR передбачає, що якщо суб'єкт даних не має реального вибору, відчуває примус до надання згоди або зазнає негативних наслідків у разі відмови, то згода не буде дійсною.[13] Якщо згода є невід'ємною частиною положень та умов, вважається, що вона не була надана вільно. Відповідно, згода не буде вважатися вільною, якщо суб'єкт даних не може відмовитися або відкликати свою згоду без шкоди для себе.[14] Поняття дисбалансу між контролером і суб'єктом даних також береться до уваги GDPR.

14. Оцінюючи, чи є згода вільно наданою, слід також брати до уваги конкретну ситуацію прив'язки згоди до договорів або надання послуг, як це описано в статті 7(4). Стаття 7(4) сформульована невичерпним чином за допомогою слів «серед іншого», що означає, що може існувати цілий ряд інших ситуацій, які охоплюються цим положенням. Загалом, будь-який елемент неналежного тиску або впливу на суб'єкта даних (який може проявлятися по-різному), що перешкоджає суб'єкту даних здійснювати свою вільну волю, робить згоду недійсною.

15. Приклад 1: Мобільний додаток для редагування фотографій просить своїх користувачів активувати GPS-локалізацію для використання його послуг. Додаток також повідомляє користувачам, що буде використовувати зібрані дані для цілей поведінкової реклами. Ані геолокалізація, ані поведінкова реклама не є необхідними для надання послуги з редагування фотографій і виходять за рамки надання основної послуги, що надається. Оскільки користувачі не можуть використовувати додаток без згоди на ці цілі, така згода не може вважатися вільно наданою.

[12] У кількох висновках Робоча група за статтею 29 дослідила межі згоди в ситуаціях, коли вона не може бути надана вільно. Це, зокрема, стосується її Висновку 15/2011 щодо визначення поняття згоди (РД 187), Робочого документа про обробку персональних даних, що стосуються здоров'я, в електронних медичних картах (РД 131), Висновку 8/2001 про обробку персональних даних у контексті працевлаштування (РД 48), та Другого висновку 4/2009 про обробку даних Всесвітнім антидопінговим агентством (ВАДА) (Міжнародний стандарт захисту приватності та особистої інформації, щодо відповідних положень Кодексу ВАДА та інших питань приватності в контексті боротьби з допінгом у спорті ВАДА та (національними) антидопінговими організаціями (РД 162).

[13] Висновок 15/2011 щодо визначення поняття згоди (РД 187), с. 12.

[14] Див. преамбули 42, 43 GDPR та Висновок 15/2011 Робочої групи за статтею 29 щодо визначення поняття згоди, ухвалений 13 липня 2011 року (РД 187), с. 12.

Прийнято

3.1.1 Дисбаланс влади

16. Преамбула 43[15] чітко вказує на те, що **органи державної влади** навряд чи можуть покладатися на згоду на обробку, оскільки, коли контролером є орган державної влади, часто існує явний дисбаланс влади у відносинах між контролером і суб'єктом даних. Також очевидно, що в більшості випадків суб'єкт даних не матиме реальних альтернатив прийняттю обробки (умов) цього контролера. EDPB вважає, що існують інші законні підстави, які загалом є більш відповідними для діяльності органів державної влади.[16]

17. Не обмежуючи цих загальних міркувань, використання згоди як законної підстави для обробки даних органами державної влади не є повністю виключеним відповідно до нормативно-правової бази GDPR. Наступні приклади показують, що використання згоди може бути доцільним за певних обставин.

18. Приклад 2: Місцевий муніципалітет планує ремонтні роботи на дорогах. Оскільки дорожні роботи можуть порушити рух транспорту на тривалий час, муніципалітет пропонує своїм громадянам можливість підписатися на електронну розсилку, щоб отримувати оновлення про хід робіт та очікувані затримки. Муніципалітет чітко пояснює, що це не є обов'язковим, і просить надати згоду на використання електронних адрес для цієї (виключної) мети. Громадяни, які не дадуть згоди, не будуть позбавлені можливості користуватися основними послугами муніципалітету або реалізовувати свої права, тому вони можуть вільно надавати або не надавати свою згоду на таке використання даних. Вся інформація про дорожні роботи також буде доступна на вебсайті муніципалітету.

19. Приклад 3: Фізична особа, яка володіє землею, потребує певних дозволів як від місцевого муніципалітету, так і від уряду провінції, у підпорядкуванні якої знаходиться муніципалітет. Обидва державні органи вимагають однакову інформацію для видачі дозволу, але не мають доступу до баз даних один одного. Тому обидва органи запитують однакову інформацію, і власник землі надсилає свої дані обом державним органам. Муніципалітет та влада провінції просять її згоди на об'єднання файлів, щоб уникнути дублювання процедур і листування. Обидва державні органи запевняють, що це не є обов'язковим і що запити на отримання дозволів все одно будуть оброблятися окремо, якщо власник вирішить не давати згоду на об'єднання своїх даних. Власник земельної ділянки може вільно надати згоду органам влади на об'єднання своїх даних.

[15] У преамбулі 43 GDPR зазначено: *«Щоб забезпечити, що згоду було надано добровільно, вона не повинна передбачати необхідність застосування дійсних законних підстав для обробки персональних даних у конкретному випадку, коли існує помітний дисбаланс між суб'єктом даних і контролером, зокрема коли контролер є органом публічної влади й, тому, малоймовірно, що згоду було надано добровільно за усіх обставин такої конкретної ситуації. (...)»*.

[16] Див. статтю 6 GDPR, зокрема пункти (1c) та (1e).

20. Приклад 4: Державна школа просить учнів дати згоду на використання їхніх фотографій у друкованому учнівському журналі. Згода в таких ситуаціях буде реальним вибором, якщо учням не буде відмовлено в освіті або послугах, і вони зможуть відмовитися від використання цих фотографій без жодної шкоди для себе.[17]

21. Дисбаланс влади також має місце в контексті **зайнятості**.[18] Враховуючи залежність, яка виникає у відносинах між роботодавцем та працівником, малоймовірно, що суб'єкт даних може відмовити роботодавцю у наданні згоди на обробку даних, не відчуваючи страху або реального ризику настання негативних наслідків у результаті відмови. Малоймовірно, що працівник зможе вільно відповісти на запит роботодавця про надання згоди, наприклад, на активацію систем моніторингу, таких як відеоспостереження на робочому місці, або на заповнення оціночних форм, не відчуваючи при цьому тиску з боку роботодавця щодо надання згоди.[19] Тому EDPB вважає проблематичним для роботодавців обробляти персональні дані нинішніх або майбутніх працівників на основі згоди, оскільки вона навряд чи буде надана добровільно. Для більшості випадків такої обробки даних на роботі законною підставою не може і не повинна бути згода працівників (стаття 6(1)(a)) через характер відносин між роботодавцем і працівником.[20]

22. Однак це не означає, що роботодавці ніколи не можуть покладатися на згоду як на законну підставу для обробки. Можуть бути ситуації, коли роботодавець може довести, що згода насправді надається вільно. Враховуючи дисбаланс влади між роботодавцем та його працівниками, працівники можуть надавати вільну згоду лише у виняткових випадках, коли це не матиме жодних негативних наслідків незалежно від того, чи нададуть вони згоду.[21]

23. Приклад 5: Знімальна група збирається проводити зйомки в певній частині офісу. Роботодавець просить усіх працівників, які сидять у цій зоні, дати згоду на зйомку, оскільки вони можуть з'явитися на задньому плані відео. Ті, хто не бажає бути знятим на відео, не караються жодним чином, а натомість отримують рівноцінні столи в іншому місці в будівлі на час зйомок.

24. Дисбаланс влади не обмежується державними органами та роботодавцями, він може виникати й в інших ситуаціях. Як підкреслює Робоча група за статтею 29 у кількох своїх висновках, згода може бути дійсною лише тоді, коли суб'єкт даних має реальний вибір, і не існує ризику обману, залякування, примусу або значних негативних наслідків (наприклад, значних додаткових витрат) у разі його відмови від згоди. Згода не буде вільною у випадках, коли існує будь-який елемент примусу, тиску або неможливості здійснити вільне волевиявлення.

---

[17] У цьому прикладі державна школа означає школу, що фінансується державою, або будь-який навчальний заклад, який за національним законодавством кваліфікується як орган державної влади чи управління.

[18] Див. також статтю 88 GDPR, де підкреслюється необхідність захисту конкретних інтересів працівників і створюється можливість для відступів у законодавстві держав-членів. Див. також преамбулу 155.

[19] Висновок 15/2011 про визначення поняття згоди (РД 187), с. 12-14, Висновок 8/2001 про обробку персональних даних у контексті зайнятості (РД 48), глава 10, Робочий документ про нагляд за електронними комунікаціями на робочому місці (РД 55), п. 4.2 та Висновок 2/2017 про обробку даних на роботі (РД 249), п. 6.2.

[20] Висновок 2/2017 щодо обробку даних на роботі, с. 6-7.

[21] Див. також Висновок 2/2017 щодо обробки даних на роботі (РД 249), пункт 6.2.

Прийнято

3.1.2 Умовність

25. Для оцінки того, чи є згода вільно наданою, важливу роль відіграє стаття 7(4) GDPR. [22]

26. Стаття 7(4) GDPR вказує, що, серед іншого, вкрай небажаною вважається ситуація «об'єднання» згоди з прийняттям умов або положень, або «прив'язка» надання договору або послуги до запиту на отримання згоди на обробку персональних даних, які не є необхідними для виконання цього договору або послуги. Якщо згода надається в такій ситуації, вважається, що вона не була надана вільно (преамбула 43). Стаття 7(4) має на меті забезпечити, щоб мета обробки персональних даних не була прихована й не була пов'язана з наданням договору або послуги, для яких ці персональні дані не є необхідними. Таким чином, GDPR гарантує, що обробка персональних даних, на яку запитується згода, не може прямо чи опосередковано стати зустрічним виконанням договору. Дві законні підстави для законної обробки персональних даних, тобто згода та договір, не можуть бути об'єднані та розмиті.

27. Примус до надання згоди на використання персональних даних, що не є суворо необхідним, обмежує вибір суб'єкта даних і перешкоджає вільній згоді. Оскільки законодавство про захист даних спрямоване на захист основоположних прав, контроль особи над своїми персональними даними є важливим, та існує вагома презумпція, що згода на обробку персональних даних, яка не є необхідною, не може розглядатися як обов'язкова винагорода в обмін на виконання договору або надання послуги.

28. Таким чином, щоразу, коли запит на отримання згоди пов'язаний із виконанням контролером договору, суб'єкт даних, який не бажає надавати свої персональні дані для обробки контролером, ризикує отримати відмову в наданні послуг, які він запитував.

29. Для того, щоб оцінити, чи має місце така ситуація пов'язаності або прив'язки, важливо визначити, яким є обсяг договору та які дані будуть необхідні для виконання цього договору.

30. Відповідно до Висновку 06/2014 Робочої групи за статтею 29, термін «необхідний для виконання договору» слід тлумачити строго. Обробка має бути необхідною для виконання договору з кожним окремим суб'єктом даних. Це може включати, зокрема, обробку адреси суб'єкта даних для доставки товарів, придбаних онлайн, або обробку даних кредитної картки для полегшення оплати. У контексті зайнятості ця підстава може дозволяти, зокрема, обробку інформації про заробітну плату та реквізитів банківських рахунків для виплати заробітної плати.[23] Між обробкою даних і метою виконання договору має бути прямий та об'єктивний зв'язок.

---

[22] Стаття 7(4) GDPR: *«Здійснюючи оцінку того, чи є згода вільно наданою, необхідно максимально враховувати те, чи залежить, між іншим, виконання договору, в тому числі надання послуги, від згоди на обробку персональних даних, що не є необхідною для виконання такого договору».* Див. також преамбулу 43 GDPR, у якій зазначено: *«[...] Презумпція ненадання добровільної згоди виникає у разі відсутності окремого дозволу на здійснення різних операцій з обробки персональних даних, попри її відповідність окремому випадку, або, якщо виконання договору, в тому числі надання послуги, залежить від надання згоди, попри те, що така згода не є обов'язковою для такого виконання».*

[23] Додаткову інформацію та приклади див. у Висновку 06/2014 щодо поняття законного інтересу контролера даних відповідно до статті 7 Директиви 95/46/ЄС, ухваленому Робочою групою за статтею 29 9 квітня 2014 року, с. 16-17. (РД 217).

Прийнято

31. Якщо контролер прагне обробити персональні дані, які насправді необхідні для виконання договору, то згода не є належною законною підставою.[24]

32. Стаття 7(4) застосовується лише тоді, коли запитувані дані **не** є необхідними для виконання договору (включаючи надання послуг), і виконання цього договору залежить від отримання цих даних на підставі згоди. І навпаки, якщо обробка **є** необхідною для виконання договору (в тому числі для надання послуги), то стаття 7(4) не застосовується.

33. Приклад 6: Банк запитує у клієнтів згоду на використання їхніх платіжних реквізитів третіми особами для цілей прямого маркетингу. Ця діяльність з обробки не є необхідною для виконання договору з клієнтом та надання звичайних послуг з обслуговування банківського рахунку. Якщо відмова клієнта надати згоду на таку обробку призведе до відмови в наданні банківських послуг, закриття банківського рахунку або, залежно від випадку, до збільшення плати за обслуговування, така згода не може бути надана вільно.

34. Вибір законодавця виділити обумовленість, серед іншого, як презумпцію відсутності свободи надання згоди, доводить, що виникнення обумовленості має бути ретельно перевірено. Термін «максимальна обережність» у статті 7(4) вказує на необхідність особливої обережності з боку контролера, коли договір (який може включати надання послуг) містить вимогу про надання згоди на обробку персональних даних, пов'язану із цим договором.

35. Оскільки формулювання статті 7(4) не тлумачиться як абсолютне, може існувати дуже обмежений простір для випадків, коли ця умова не зробить згоду недійсною. Однак слово «презумпція» в преамбулі 43 чітко вказує на те, що такі випадки будуть вкрай винятковими.

36. У будь-якому випадку, тягар доведення у статті 7(4) лежить на контролері.[25] Це конкретне правило відображає загальний принцип підзвітності, який пронизує весь GDPR. Однак, коли застосовується стаття 7(4), контролеру буде складніше довести, що згоду було надано суб'єктом даних вільно.[26]

37. Контролер міг би стверджувати, що його організація пропонує суб'єктам даних реальний вибір, якби вони могли вибирати між послугою, яка передбачає згоду на використання персональних даних для додаткових цілей, з одного боку, та еквівалентною послугою, яку пропонує той самий контролер, але яка не передбачає надання згоди на використання даних для додаткових цілей, з іншого боку. Якщо існує можливість виконання договору або надання передбаченої договором послуги цим контролером без згоди на інше або додаткове використання даних, це означає, що умовна послуга більше не є умовною. Однак обидві послуги повинні бути дійсно еквівалентними.

---

[24] Тоді відповідною нормативно-правовою базою може бути стаття 6(1)(b) (договір).

[25] Див. також статтю 7(1) GDPR, у якій зазначено, що контролер повинен довести, що згоду суб'єкта даних було надано вільно.

[26] Певною мірою, введення цього пункту є кодифікацією існуючих настанов Робочої групи за статтею 29. Як зазначено у Висновку 15/2011, коли суб'єкт даних перебуває в ситуації залежності від контролера даних — через характер відносин або особливі обставини — може існувати вагома презумпція того, що свобода надання згоди в таких контекстах обмежена (наприклад, у трудових відносинах або якщо збір даних здійснюється державним органом). З набуттям чинності статтею 7(4) контролеру буде складніше довести, що згоду було надано суб'єктом даних вільно. Див: Висновок 15/2011 Робочої групи за статтею 29 щодо визначення поняття згоди (РД 187), с. 12-17.
Прийнято

38. EDPB вважає, що згоду не можна вважати вільно наданою, якщо контролер стверджує, що існує вибір між його послугою, яка включає згоду на використання персональних даних для додаткових цілей, з одного боку, та еквівалентною послугою, що пропонується іншим контролером, з іншого боку. У такому випадку свобода вибору буде поставлена в залежність від того, що роблять інші учасники ринку, а також від того, чи вважатиме суб'єкт персональних даних послуги іншого контролера дійсно еквівалентними. Крім того, це означатиме обов'язок контролерів стежити за розвитком ринку, щоб забезпечити постійну чинність згоди на обробку даних, оскільки конкурент може змінити свою послугу на більш пізньому етапі. Отже, використання цього аргументу означає, що згода, яка покладається на альтернативний варіант, запропонований третьою стороною, не відповідає GDPR, а це означає, що постачальник послуг не може перешкоджати суб'єктам даних у доступі до послуги на підставі того, що вони не дають на це згоди.

39. Для того, щоб згода була вільно надана, доступ до послуг та функцій не повинен залежати від згоди користувача на зберігання інформації або отримання доступу до вже збереженої інформації в термінальному обладнанні користувача (так звані «бар'єри файлів cookie»)[27].

40. Приклад 6а: Провайдер вебсайту впроваджує скрипт, який блокує доступ до контенту, за винятком запиту на прийняття файлів cookie та інформації про те, які саме файли cookie встановлюються та з якою метою будуть оброблятися дані. Неможливо отримати доступ до контенту без натискання кнопки «Прийняти файли cookie». Оскільки суб'єкт даних не має реального вибору, його згода не є вільно наданою.

41. Це не є дійсною згодою, оскільки надання послуги залежить від натискання суб'єктом даних кнопки «Прийняти файли cookie». Йому не надається реальний вибір.

3.1.3 Деталізація

42. Послуга може включати кілька операцій з обробки для більш ніж однієї мети. У таких випадках суб'єкти даних повинні мати можливість вільно обирати, на яку мету вони погоджуються, а не давати згоду на сукупність цілей обробки. У певному випадку для того, щоб почати пропонувати послугу, може знадобитися кілька згод відповідно до GDPR.

43. Стаття 43 роз'яснює, що вважається, що згода не була надана вільно, якщо процес/процедура отримання згоди не дозволяє суб'єктам даних надавати окрему згоду на операції з обробки персональних даних відповідно (наприклад, тільки на деякі операції з обробки, але не на інші), попри те, що це є доцільним в кожному конкретному випадку. У преамбулі 32 зазначено: *«Згода повинна поширюватися на всі види обробки, що здійснюються з однією і тією ж метою або цілями. Якщо обробка переслідує декілька цілей, згода повинна бути надана на всі ці цілі».*

44. Якщо контролер об'єднав кілька цілей обробки й не намагався отримати окрему згоду на кожну з них, це свідчить про відсутність вільного вибору. Така деталізація тісно пов'язана з необхідністю того, щоб згода була конкретною, як обговорюється в розділі 3.2 нижче. Коли обробка даних здійснюється для досягнення кількох цілей, рішенням для дотримання умов дійсної згоди є деталізація, тобто розділення цих цілей та отримання згоди на кожну з них.

[27] Таким чином, як пояснювалося вище, умови GDPR щодо отримання дійсної згоди застосовуються в ситуаціях, що підпадають під дію Директиви про приватність та електронні комунікації.

45. Приклад 7: У тому самому запиті на отримання згоди роздрібний торговець просить своїх клієнтів надати згоду на використання їхніх даних для надсилання їм маркетингових повідомлень електронною поштою, а також на передачу їхніх даних іншим компаніям, що входять до їхньої групи. Ця згода не є деталізованою, оскільки немає окремих згод для цих двох окремих цілей, тому згода не буде дійсною. У цьому випадку необхідно отримати окрему згоду на надсилання контактних даних комерційним партнерам. Така окрема згода буде вважатися дійсною для кожного партнера (див. також розділ 3.3.1), ідентифікаційні дані якого були надані суб'єкту даних під час збору його згоди, якщо вони надсилаються їм з однією і тією ж метою (у цьому прикладі — з маркетинговою метою).

3.1.4 Шкода

46. Контролер повинен довести, що відмова або відкликання згоди можливе без шкоди (преамбула 42). Наприклад, контролер повинен довести, що відкликання згоди не призведе до жодних витрат для суб'єкта даних і, таким чином, не спричинить явної шкоди для тих, хто відкликає згоду.

47. Іншими прикладами шкоди є обман, залякування, примус або значні негативні наслідки, якщо суб'єкт даних не дає згоду. Контролер повинен мати можливість довести, що суб'єкт даних мав вільний або реальний вибір щодо того, чи давати згоду, і що була можливість відкликати згоду без шкоди для нього.

48. Якщо контролер може довести, що послуга передбачає можливість відкликання згоди без будь-яких негативних наслідків, наприклад, без погіршення якості послуги на шкоду користувачеві, це може слугувати доказом того, що згоду було надано вільно. GDPR не виключає всіх заохочень, але тягар доведення того, що згоду було надано вільно за всіх обставин, лежить на контролері.

49. Приклад 8: Під час завантаження мобільного додатку для моніторингу способу життя додаток запитує згоду на доступ до акселерометра телефону. Це не є необхідним для роботи програми, але корисно для контролера, який хоче дізнатися більше про рухи та рівень активності своїх користувачів. Коли користувач пізніше відкликає цю згоду, він дізнається, що додаток тепер працює лише в обмеженому обсязі. Це приклад шкоди, про яку йдеться в преамбулі 42, що означає, що згода ніколи не була отримана належним чином (а отже, контролер повинен видалити всі персональні дані про пересування користувачів, зібрані в такий спосіб).

50. Приклад 9: Суб'єкт даних підписується на розсилку новин від роздрібного продавця модного одягу із загальними знижками. Роздрібний торговець просить у суб'єкта даних згоди на збір додаткових даних про його вподобання щодо покупок, щоб адаптувати пропозиції до його вподобань на основі історії покупок або анкети, яку він заповнює добровільно. Коли суб'єкт даних пізніше відкликає згоду, він знову отримає неперсоніфіковані знижки на модний одяг. Це не є шкодою, оскільки було втрачено лише допустиме заохочення.

51. Приклад 10: Модний журнал пропонує читачам доступ до купівлі нових засобів для макіяжу до офіційного запуску.

52. Незабаром ці продукти з'являться у продажу, але читачам журналу пропонується ексклюзивний попередній перегляд цих продуктів. Для того, щоб скористатися цією перевагою, люди повинні вказати свою поштову адресу та погодитися на підписку в списку розсилки журналу. Поштова адреса необхідна для доставки, а список розсилки використовується для надсилання комерційних пропозицій на такі товари, як косметика або футболки, протягом усього року.

Прийнято

53. Компанія пояснює, що дані списку розсилки будуть використовуватися лише для розсилки товарів і паперової реклами самим журналом і не будуть передані жодній іншій організації.

54. Якщо читач не хоче розкривати свою адресу з цієї причини, це не завдасть йому шкоди, оскільки продукція все одно буде йому доступна.

3.2 Конкретні цілі

55. Стаття 6(1)(a) підтверджує, що згода суб'єкта даних повинна бути надана щодо «однієї або декількох конкретних» цілей і що суб'єкт даних має право вибору щодо кожної з них.[28] Вимога, що згода має бути *«конкретною»*, має на меті забезпечити певний ступінь контролю користувача та прозорості для суб'єкта даних. Ця вимога не була змінена GDPR і залишається тісно пов'язаною з вимогою «інформованої» згоди. Водночас вона повинна тлумачитися відповідно до вимоги «деталізації» для отримання «вільної» згоди.[29] Таким чином, для дотримання елементу «конкретності» контролер має застосувати:

    i конкретизацію мети як запобіжник проти «розмитості функцій»;

    ii деталізацію запитів на отримання згоди; та

    iii чітке відокремлення інформації, пов'язаної з отриманням згоди на обробку даних, від інформації з інших питань.

56. **Додатково до пункту (i):** Відповідно до статті 5(1)(b) GDPR, отриманню дійсної згоди завжди передує визначення конкретної, чіткої та законної мети запланованої діяльності з обробки даних.[30] Необхідність отримання конкретної згоди в поєднанні з поняттям обмеження мети в статті 5(1)(b) слугує захистом від поступового розширення або розмивання цілей, для яких обробляються дані, після того, як суб'єкт даних дав згоду на початковий збір даних. Це явище, також відоме як «розмитість функцій», становить ризик для суб'єктів даних, оскільки може призвести до непередбачуваного використання персональних даних контролерами.

---

[28] Подальші вказівки щодо визначення «цілей» можна знайти у Висновку 3/2013 щодо обмеження цілей (РД 203).

[29] У преамбулі 3 GDPR зазначено, що окрема згода на різні операції з обробки даних буде необхідна у всіх випадках, коли це доцільно.
Необхідно передбачити варіанти деталізованої згоди, щоб дозволити суб'єктам даних надавати згоду окремо на окремі цілі.

[30] Висновок 3/2013 Робочої групи за статтею 29 щодо обмеження цілей (РД 203), с. 16: *«Із цих причин мета, яка є нечіткою або загальною, наприклад, «покращення досвіду користувачів», «маркетингові цілі», «цілі IT-безпеки» або «майбутні дослідження», як правило, не буде відповідати критерію «конкретності», якщо вона не буде деталізована».*
Прийнято

57. Якщо контролер покладається на статтю 6(1)(a), суб'єкти даних завжди повинні надавати згоду на конкретну мету обробки.[31] Відповідно до концепції *обмеження цілей*, статті 5(1)(b) та преамбули 32, згода може охоплювати різні операції, якщо ці операції слугують одній меті. Зрозуміло, що конкретна згода може бути отримана лише тоді, коли суб'єкти даних конкретно поінформовані про передбачувані цілі використання даних, які їх стосуються.

58. Попри положення про сумісність цілей, згода повинна бути конкретною щодо мети. Суб'єкти даних надають свою згоду з розумінням того, що вони контролюють ситуацію і що їхні дані будуть оброблятися лише для зазначених цілей. Якщо контролер обробляє дані на основі згоди й бажає обробляти дані також для іншої мети, він повинен отримати додаткову згоду на цю іншу мету, якщо тільки не існує іншої законної підстави, яка краще відображає ситуацію.

59. Приклад 11: Мережа кабельного телебачення збирає персональні дані абонентів на основі їхньої згоди, щоб надавати їм персональні пропозиції щодо нових фільмів, які можуть їх зацікавити, виходячи з їхніх глядацьких звичок. Через деякий час телеканал вирішує, що він хотів би дозволити третім сторонам надсилати (або показувати) таргетовану рекламу на основі глядацьких уподобань абонентів. З огляду на цю нову мету, потрібна нова згода.

60. **Додатково до пункту (ii):** Механізми отримання згоди повинні бути не лише деталізованими, щоб відповідати вимозі «вільної», але й елементу «конкретності». Це означає, що контролер, який запитує згоду для різних цілей, повинен надавати окрему згоду для кожної мети, щоб користувачі могли надавати конкретну згоду для конкретних цілей.

61. **Додатково до пункту (iii):** Зрештою, контролери повинні надавати конкретну інформацію з кожним окремим запитом на згоду про дані, які обробляються для кожної мети, щоб суб'єкти даних знали про вплив різних варіантів вибору, які вони мають. Таким чином, суб'єкти даних отримують можливість надавати конкретну згоду. Це питання перетинається з вимогою про те, що контролери повинні надавати чітку інформацію, як обговорюється в пункті 3.3. нижче.

3.3 Інформована згода

62. GDPR посилює вимогу про те, що згода має бути інформованою. Відповідно до статті 5 GDPR, вимога прозорості є одним із основоположних принципів, тісно пов'язаних із принципами справедливості та законності. Надання інформації суб'єктам даних до отримання їхньої згоди має важливе значення для того, щоб вони могли приймати поінформовані рішення, розуміти, на що вони погоджуються, і, наприклад, реалізувати своє право відкликати свою згоду. Якщо контролер не надає доступної інформації, контроль користувача стає ілюзорним, а згода буде недійсною підставою для обробки.

63. Наслідком недотримання вимог щодо інформованої згоди є те, що згода буде недійсною, а контролер може порушити статтю 6 GDPR.

[31] Це узгоджується з Висновком 15/2011 Робочої групи за статтею 29 щодо визначення поняття згоди (РД 187), зокрема, на с. 17.

3.3.1 Мінімальні вимоги до змісту згоди, щоб вона вважалася «інформованою»

64. Для того, щоб згода вважалася інформованою, необхідно поінформувати суб'єкта даних про певні умови, які мають вирішальне значення для здійснення вибору. Тому EDPB вважає, що для отримання дійсної згоди необхідна щонайменше така інформація:

i. особа контролера;[32]

ii. мета кожної операції з обробки, на яку запитується згода;[33]

iii. які (тип) дані будуть збиратися та використовуватися;[34]

iv. iv. наявність права на відкликання згоди;[35]

v. інформація про використання даних для автоматизованого прийняття рішень відповідно до статті 22(2)(c)[36], де це доцільно; та

vi. можливі ризики передачі даних через відсутність необхідного рішення та відповідних гарантій, як описано в статті 46.[37]

65. Щодо пунктів (i) та (iii), EDPB зазначає, що у випадку, коли згода, яка запитується, має бути отримана від декількох (спільних) контролерів або якщо дані мають бути передані або оброблені іншими контролерами, які бажають покладатися на первинну згоду, всі ці організації повинні бути зазначені. Оператори не повинні бути зазначені в рамках вимог до надання згоди, хоча для дотримання статей 13 і 14 GDPR контролери повинні будуть надати повний список одержувачів або категорій одержувачів, включаючи операторів. На завершення, EDPB зазначає, що залежно від обставин та контексту справи може знадобитися більше інформації, щоб дозволити суб'єкту даних по-справжньому зрозуміти операції з обробки даних, про які йдеться.

---

[32] Див. також преамбулу 42 GDPR: *«[...] Для того, щоб згода вважалася поінформованою, суб'єкт даних повинен бути обізнаним принаймні про особу контролера та цілі обробки, для яких призначено використання персональних даних. [...]»*

[33] Там же, див. преамбулу 42 GDPR.

[34] Див. також Висновок 15/2011 Робочої групи за статтею 29 щодо визначення поняття згоди (РД 187), с. 19-20.

[35] Див. статтю 7(3) GDPR.

[36] Див. також Настанови Робочої групи за статтею 29 щодо автоматизованого прийняття індивідуальних рішень та профілювання для цілей Регламенту 2016/679 (РД 251), пункт IV.B, с. 20 і далі.

[37] Відповідно до статті 49(1)(a), коли запитується явна згода, необхідна конкретна інформація про відсутність гарантій, описаних у статті 46. Див. також Висновок 15/2011 Робочої групи за статтею 29 щодо визначення поняття згоди (РД 187), с. 19.

3.3.2 Як надавати інформацію

66. GDPR не встановлює форму або спосіб, у якому інформація повинна бути надана для виконання вимоги щодо інформованої згоди. Це означає, що достовірна інформація може бути представлена різними способами, наприклад, у вигляді письмових або усних заяв, аудіо- чи відеоповідомлень. Однак GDPR встановлює кілька вимог до інформованої згоди, в основному в статті 7(2) та преамбулі 32. Це призводить до вищих стандартів щодо ясності та доступності інформації.

67. Запитуючи згоду, контролери повинні переконатися, що вони використовують чітку та зрозумілу мову в усіх випадках. Це означає, що повідомлення має бути зрозумілим для пересічної людини, а не лише для юристів. Контролери не можуть використовувати довгі політики конфіденційності, які важко зрозуміти, або заяви, повні юридичного жаргону. Згода має бути чіткою та відрізнятися від інших питань, а також надаватися у зрозумілій та доступній формі. Ця вимога, загалом, означає, що інформація, важлива для прийняття обґрунтованого рішення про надання згоди, не може бути прихована в загальних положеннях та умовах.[38]

68. Контролер повинен забезпечити, щоб згода надавалася на основі інформації, яка дозволяє суб'єктам даних легко ідентифікувати, хто є контролером, та зрозуміти, на що вони погоджуються. Контролер повинен чітко описати мету обробки даних, на яку запитується згода.[39]

69. Інші конкретні вказівки щодо доступності містяться в настановах Робочої групи за статтею 29 щодо прозорості. Якщо згода надається за допомогою електронних засобів, запит має бути чітким і стислим. Багаторівнева та деталізована інформація може бути відповідним способом виконання подвійного зобов'язання — бути точною та повною, з одного боку, та зрозумілою, з іншого боку.

70. Контролер повинен оцінити, яка саме аудиторія надає персональні дані його організації. Наприклад, якщо цільова аудиторія включає неповнолітніх суб'єктів даних, контролер повинен переконатися, що інформація є зрозумілою для неповнолітніх.[40] Визначивши свою аудиторію контролери повинні визначити, яку інформацію вони повинні надавати, і, відповідно, як вони будуть представляти цю інформацію суб'єктам даних.

---

[38] Заява про надання згоди має називатися саме так. Формулювання на кшталт «Я знаю, що...» не відповідають вимогам чіткої мови.

[39] Див. статті 4(11) та 7(2) GDPR.

[40] Див. також преамбулу 58 щодо інформації, зрозумілої для дітей.

71. Стаття 7(2) стосується попередньо сформульованих письмових заяв про згоду, які також стосуються інших питань. Якщо згода запитується як частина (паперового) договору, запит на згоду повинен бути чітко відокремлений від інших питань. Якщо паперовий договір містить багато аспектів, які не пов'язані з питанням надання згоди на використання персональних даних, питання згоди має бути чітко виокремлене або винесене в окремий документ. Аналогічно, якщо згода запитується за допомогою електронних засобів, запит на згоду повинен бути окремим і чітким, він не може бути просто пунктом в умовах, відповідно до преамбули 32. [41] Для пристосування до невеликих екранів або ситуацій з обмеженим простором для інформації можна розглянути можливість багаторівневого представлення інформації, де це доцільно, щоб уникнути надмірного порушення користувацького досвіду або дизайну продукту.

72. Контролер, який покладається на згоду суб'єкта даних, повинен також мати справу з окремими інформаційними обов'язками, викладеними в статтях 13 і 14, щоб відповідати вимогам GDPR. На практиці дотримання обов'язків щодо надання інформації та дотримання вимоги про інформовану згоду в багатьох випадках може призвести до інтегрованого підходу. Однак цей розділ написаний з розумінням того, що дійсна «інформована» згода може існувати, навіть якщо не всі пункти статей 13 та/або 14 згадуються в процесі отримання згоди (ці моменти, звичайно, повинні бути згадані в інших місцях, наприклад, у повідомленні про конфіденційність компанії). Робоча група за статтею 29 випустила окремі настанови щодо вимоги прозорості.

73. Приклад 12: Компанія X є контролером, який отримав скарги на те, що суб'єктам даних незрозуміло, для яких цілей використання даних їх просять надати згоду. Компанія вважає за необхідне перевірити, чи зрозуміла суб'єктам даних інформація, викладена в запиті на отримання згоди. Компанія X організовує добровільні тестові групи з певних категорій своїх клієнтів і представляє нові оновлення інформації про згоду цим тестовим аудиторіям перед тим, як поширювати її назовні. Відбір групи відбувається з дотриманням принципу незалежності та на основі стандартів, що забезпечують репрезентативність та неупередженість результатів. Група експертів отримує анкету та вказує, що вони зрозуміли з інформації та як би вони оцінили її з точки зору зрозумілості та релевантності інформації. Контролер продовжує тестування до тих пір, поки групи не вкажуть, що інформація є зрозумілою. Компанія X складає звіт про тестування та зберігає його для подальшого використання. Цей приклад показує можливий спосіб для компанії X довести, що суб'єкти даних отримували чітку інформацію перед тим, як дати згоду на обробку персональних даних компанією X.

[41] Див. також преамбулу 42 та Директиву 93/13/ЄС, зокрема, статтю 5 (проста зрозуміла мова, у разі сумнівів тлумачення на користь споживача) та статтю 6 (недійсність несправедливих умов, договір продовжує існувати без цих умов, якщо вони все ще є розумними, в іншому випадку весь договір є недійсним).

Прийнято

74. Приклад 13: Компанія здійснює обробку даних на основі згоди. Компанія використовує багаторівневе повідомлення про конфіденційність, яке містить запит на отримання згоди. Компанія розкриває всі основні відомості про контролера та передбачену діяльність з обробки даних.[42] Однак у першому інформаційному шарі повідомлення компанія не вказує, як можна зв'язатися з відповідальним за захист даних. Для того, щоб мати дійсну законну підставу, як зазначено в статті 6, цей контролер отримав дійсну «інформовану» згоду, навіть якщо контактні дані відповідального за захист даних не були повідомлені суб'єкту даних (у першому інформаційному шарі), відповідно до статті 13(1)(b) або 14(1)(b) GDPR.

3.4 Однозначне формулювання побажань

75. GDPR чітко визначає, що згода вимагає заяви суб'єкта даних або чіткого стверджувального акту, що означає, що вона завжди повинна бути надана шляхом ствердної дії або заяви. Повинно бути очевидно, що суб'єкт даних дав згоду на конкретну обробку.

76. Стаття 2(h) Директиви 95/46/ЄС описує згоду як «висловлення побажань, за допомогою яких суб'єкт даних висловлює свою згоду на обробку персональних даних, що стосуються його». Стаття 4(11) GDPR ґрунтується на цьому визначенні, уточнюючи, що дійсна згода вимагає *однозначної* вказівки за допомогою *заяви або чіткої ствердної дії*, відповідно до попередніх рекомендацій, виданих Робочою групою за статтею 29.

77. «Чітка ствердна дія» означає, що суб'єкт даних повинен був здійснити навмисну дію, щоб дати згоду на конкретну обробку.[43] У преамбулі 32 викладені додаткові вказівки щодо цього. Згода може бути отримана шляхом письмової або (записаної) усної заяви, в тому числі за допомогою електронних засобів.

78. Можливо, найбільш буквальним способом виконання критерію «письмової заяви» є забезпечення того, щоб суб'єкт даних написав листа або надіслав електронного листа контролеру, пояснюючи, на що саме він погоджується. Однак часто це не є реалістичним. Письмові заяви можуть бути різних форм і розмірів, які можуть відповідати вимогам GDPR.

---

[42] Зауважте, що коли особа контролера або мета обробки не є очевидними з першого інформаційного рівня багаторівневого повідомлення про конфіденційність (і розташовані на наступних підрівнях), контролеру даних буде важко довести, що суб'єкт даних надав інформовану згоду, якщо тільки він не зможе довести, що суб'єкт даних отримав доступ до цієї інформації до того, як надав згоду.

[43] Див. Робочий документ персоналу Комісії «Оцінка впливу», Додаток 2, с. 20, а також с. 105-106: *«Як також зазначено у висновку, прийнятому Робочою групою за статтею 29 щодо згоди, видається важливим роз'яснити, що дійсна згода вимагає використання механізмів, які не залишають сумнівів у намірі суб'єкта даних дати згоду, водночас чітко пояснюючи, що — в контексті онлайн-середовища — використання опцій за замовчуванням, які суб'єкт даних повинен змінити, щоб відхилити обробку («згода, що ґрунтується на мовчанні»), саме по собі не становить однозначної згоди. Це дасть особам більше контролю над власними даними, коли обробка ґрунтується на їхній згоді. Що стосується впливу на контролерів даних, то він не матиме значного впливу, оскільки лише уточнює та краще описує наслідки чинної Директиви щодо умов отримання дійсної та змістовної згоди від суб'єкта даних. Зокрема, оскільки «явна» згода роз'яснює — замість «однозначної» — умови та якість згоди та не має на меті розширити випадки та ситуації, в яких (явна) згода повинна використовуватися як підстава для обробки, вплив цього заходу на контролерів даних не очікується значним».*
Прийнято

79. Не обмежуючи чинного (національного) договірного права, згода може бути отримана за допомогою записаної усної заяви, хоча перед наданням згоди необхідно належним чином врахувати інформацію, доступну суб'єкту даних. Використання попередньо відмічених полів для надання згоди є недійсним відповідно до GDPR. Мовчання або бездіяльність з боку суб'єкта даних, а також просте продовження надання послуги не можуть розглядатися як активне вираження вибору.

80. Приклад 14: Під час встановлення програмного забезпечення програма запитує у суб'єкта даних згоду на використання незнеособлених звітів про збої для покращення програмного забезпечення. Запит на згоду супроводжується багаторівневим повідомленням про конфіденційність, що містить необхідну інформацію. Активно відмічаючи опціональне поле з написом «Я згоден», користувач має змогу здійснити «чіткий стверджувальний акт», щоб дати згоду на обробку даних.

81. Контролер повинен також пам'ятати, що згода не може бути отримана за допомогою тієї самої дії, що й згода на укладення договору або прийняття загальних умов надання послуг. Беззастережне прийняття загальних положень та умов не може розглядатися як чітка ствердна дія щодо надання згоди на використання персональних даних. GDPR не дозволяє контролерам пропонувати попередньо відмічені поля або конструкції відмови, які вимагають втручання суб'єкта даних, щоб запобігти згоді (наприклад, «поля для відмови»). [44]

82. Якщо згода має бути надана після запиту за допомогою електронних засобів, запит на згоду не повинен *надмірно* перешкоджати використанню послуги, на яку надається згода. [45] Активна стверджувальна дія, за допомогою якої суб'єкт даних висловлює свою згоду, може бути необхідною, якщо менш нав'язливий або менш обтяжливий спосіб може спричинити неоднозначність. Таким чином, може бути необхідним, щоб запит на згоду певною мірою переривав процес використання, щоб зробити цей запит ефективним.

83. Однак, у рамках вимог GDPR, контролери мають свободу розробляти процес отримання згоди, який підходить для їхньої організації. У зв'язку із цим фізичні рухи можна кваліфікувати як чітку ствердну дію відповідно до GDPR.

84. Контролери повинні розробляти механізми отримання згоди таким чином, щоб вони були зрозумілими для суб'єктів даних. Контролери повинні уникати двозначності та гарантувати, що дію, за допомогою якої надається згода, можна відрізнити від інших дій. Таким чином, просте продовження звичайного використання вебсайту не є поведінкою, з якої можна зробити висновок про бажання суб'єкта даних висловити свою згоду на запропоновану операцію з обробки.

[44] Див. статтю 7(2). Див. також Робочий документ 02/2013 про отримання згоди на використання файлів cookie (РД 208), с. 3-6.

[45] Див. преамбулу 32 GDPR.

85. Приклад 15: Проведення пальцем по смужці на екрані, відмова перед смарт-камерою, поворот смартфона за годинниковою стрілкою або рух у вигляді вісімки можуть бути варіантами вираження згоди, якщо надається чітка інформація та зрозуміло, що відповідний рух означає згоду на конкретний запит (наприклад, якщо ви проведете пальцем по цій смужці вліво, ви погоджуєтеся на використання інформації X для мети Y. Повторіть рух для підтвердження»). Контролер повинен довести, що згоду було отримано саме в такий спосіб, а суб'єкти даних повинні мати можливість відкликати згоду так само легко, як її було надано.

86. Приклад 16: Виходячи з преамбули 32, такі дії, як прокручування або перегортання вебсторінки або подібні дії користувача за жодних обставин не задовольняють вимогу чіткої та ствердної дії: такі дії може бути важко відрізнити від іншої діяльності або взаємодії користувача, а отже, визначити, що однозначна згода була отримана, також буде неможливо. Крім того, в такому випадку, користувачеві буде складно надати можливість відкликати згоду так само легко, як і надати її.

87. У цифровому контексті багато послуг потребують персональних даних для функціонування, отже, суб'єкти даних щодня отримують численні запити на згоду, які потребують відповідей за допомогою кліків та свайпів. Це може призвести до певної «втоми від кліків»: коли з ними стикаються занадто часто, фактичний попереджувальний ефект механізмів надання згоди зменшується.

88. Це призводить до ситуації, коли питання про згоду більше не читаються. Це становить особливий ризик для суб'єктів даних, оскільки, як правило, згода запитується на дії, які загалом є незаконними без їхньої згоди. GDPR покладає на контролерів обов'язок розробити способи вирішення цієї проблеми.

89. Часто згадуваним прикладом для цього в онлайн-контексті є отримання згоди інтернет-користувачів через налаштування їхніх браузерів. Такі налаштування повинні бути розроблені відповідно до умов дійсної згоди в GDPR, наприклад, що згода повинна бути деталізованою для кожної з передбачених цілей і що інформація, яка надається, повинна містити ім'я контролерів.

90. У будь-якому випадку, згода завжди повинна бути отримана до того, як контролер почне обробляти персональні дані, для яких потрібна згода. У своїх висновках Робоча група за статтею 29 послідовно дотримується думки, що згоду слід надавати до початку діяльності з обробки.[46] Хоча GDPR буквально не передбачає в статті 4(11), що згода повинна бути надана до початку обробки, це явно мається на увазі. Заголовок статті 6(1) та формулювання «надав» у статті 6(1)(a) підтримують таке тлумачення. Зі статті 6 та преамбули 40 логічно випливає, що перед початком обробки даних повинна бути наявна дійсна законна підстава. Таким чином, згода повинна бути надана до початку обробки даних. У цілому, може бути достатньо запитати згоду суб'єкта даних один раз. Однак контролери повинні отримати нову та конкретну згоду, якщо цілі обробки даних змінюються після отримання згоди або якщо передбачається додаткова мета.

[46] Робоча група за статтею 29 послідовно дотримується цієї позиції, починаючи з Висновку 15/2011 щодо визначення поняття згоди (РД 187), с. 30-31.

4 ОТРИМАННЯ ЯВНОЇ ЗГОДИ

91. Явна згода необхідна в певних ситуаціях, коли виникає серйозний ризик для захисту даних, а отже, коли високий рівень індивідуального контролю над персональними даними вважається доцільним. Відповідно до GDPR, явна згода відіграє певну роль у статті 9 про обробку спеціальних категорій даних, положеннях про передачу даних третім країнам або міжнародним організаціям за відсутності належних гарантій у статті 49[47], а також у статті 22 про автоматизоване прийняття індивідуальних рішень, у тому числі про профайлінг.[48]

92. GDPR передбачає, що «заява або чітка ствердна дія» є необхідною умовою для надання «звичайної» згоди. Оскільки вимога «звичайної» згоди в GDPR вже піднята на вищий рівень порівняно з вимогою згоди в Директиві 95/46/ЄС, необхідно роз'яснити, яких додаткових зусиль повинен докласти контролер, щоб отримати *явну* згоду суб'єкта даних відповідно до GDPR.

93. Термін *«явна»* стосується способу вираження згоди суб'єктом даних. Це означає, що суб'єкт даних повинен дати пряму заяву про згоду. Очевидним способом переконатися в тому, що згода є явною, є пряме підтвердження згоди в письмовій заяві. За необхідності, контролер може переконатися, що письмова заява підписана суб'єктом даних, щоб усунути всі можливі сумніви та потенційний брак доказів у майбутньому.[49]

94. Однак така підписана заява не є єдиним способом отримати явну згоду, і не можна сказати, що GDPR вимагає письмової та підписаної заяви за всіх обставин, які вимагають дійсної явної згоди. Наприклад, у цифровому або онлайн контексті суб'єкт даних може зробити необхідну заяву, заповнивши електронну форму, надіславши електронного листа, завантаживши відсканований документ із підписом суб'єкта даних або використавши електронний підпис. Теоретично, використання усних заяв також може бути достатньо явним для отримання дійсної явної згоди, однак, контролеру може бути важко довести, що всі умови дійсної явної згоди були дотримані під час запису заяви.

---

[47] Згідно зі статтею 49 (1)(a) GDPR, явна згода може зняти заборону на передачу даних до країн, які не мають належного рівня законодавства щодо захисту даних. Також зверніть увагу на Робочий документ щодо спільного тлумачення статті 26(1) Директиви 95/46/ЄС від 24 жовтня 1995 року (РД 114), с. 11, де Робоча група за статтею 29 вказала, що згода на передачу даних, яка відбувається періодично або на постійній основі, є недоцільною.

[48] У статті 22 GDPR вводить положення про захист суб'єктів даних від прийняття рішень, заснованих виключно на автоматизованій обробці, включаючи профайлінг. Рішення, прийняті на цій основі, дозволені за певних правових умов. Згода відіграє ключову роль у цьому механізмі захисту, оскільки стаття 22(2)(c) GDPR чітко визначає, що контролер може продовжувати автоматизоване прийняття рішень, включаючи профайлінг, який може суттєво вплинути на особу, за умови явної згоди суб'єкта даних. Робоча група за статтею 29 розробила окремі настанови із цього питання: Настанови Робочої групи за статтею 29 щодо автоматизованого прийняття рішень та профайлінгу для цілей Регламенту 2016/679, 3 жовтня 2017 року (РД 251).

[49] Див. також Висновок 15/2011 Робочої групи за статтею 29 щодо визначення поняття згоди (РД 187), с. 25.

Прийнято

95. Організація також може отримати явну згоду за допомогою телефонної розмови, за умови, що інформація про вибір є справедливою, зрозумілою та чіткою, і вона просить суб'єкта даних надати конкретне підтвердження (наприклад, натиснути кнопку або надати усне підтвердження).

96. Приклад 17: Контролер даних може також отримати явну згоду від відвідувача свого вебсайту, запропонувавши йому вікно явної згоди, яке містить прапорці «Так» і «Ні», за умови, що текст чітко вказує на згоду, наприклад, «Цим я даю згоду на обробку моїх даних», а не, наприклад, «Мені зрозуміло, що мої дані будуть оброблятися». Само собою зрозуміло, що мають бути дотримані умови інформованої згоди, а також інші умови для отримання дійсної згоди.

97. Приклад 18: Клініка косметичної хірургії шукає явну згоду пацієнта на передачу його медичної картки експерту, який має отримати другу думку про стан пацієнта. Медична картка — це цифровий файл. З огляду на специфічний характер відповідної інформації, клініка просить електронний підпис суб'єкта даних, щоб отримати дійсну явну згоду та мати можливість довести, що явна згода була отримана.[50]

98. Двоетапна перевірка згоди також може бути способом переконатися в тому, що явна згода є дійсною. Наприклад, суб'єкт даних отримує електронного листа з повідомленням про намір контролера обробляти запис, що містить медичні дані. Контролер пояснює в електронному листі, що він просить надати згоду на використання певного набору інформації з конкретною метою. Якщо суб'єкт даних погоджується на використання цих даних, контролер просить його надіслати відповідь електронною поштою, що містить твердження «Я згоден». Після відправлення відповіді суб'єкт даних отримує посилання для підтвердження, на яке необхідно перейти, або SMS-повідомлення з кодом підтвердження, щоб підтвердити згоду.

99. Стаття 9(2) не визнає згоду, «необхідну для виконання договору», як виняток із загальної заборони на обробку спеціальних категорій даних. Тому контролери та держави-члени ЄС, які стикаються з такою ситуацією, повинні вивчити конкретні винятки в підпунктах (b)-(j) статті 9(2). Якщо жоден із винятків (b)-(j) не застосовується, єдиним можливим законним винятком для обробки таких даних залишається отримання явної згоди відповідно до умов дійсної згоди в GDPR.

[50] Цей приклад не впливає на Регламент ЄС № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку.

Прийнято

100. Приклад 19: Авіакомпанія Holiday Airways пропонує послугу супроводу для пасажирів, які не можуть подорожувати без сторонньої допомоги, наприклад, через інвалідність. Клієнт бронює квиток на рейс з Амстердама до Будапешта і просить надати йому допомогу, щоб він зміг потрапити на борт літака. Авіакомпанія Holiday Airways вимагає від неї надати інформацію про стан її здоров'я, щоб мати змогу організувати для неї відповідні послуги (отже, є багато можливостей, наприклад, інвалідний візок біля виходу на посадку або асистент, який подорожує з нею з пункту А в пункт Б). Holiday Airways просить надати явну згоду на обробку даних про стан здоров'я цього клієнта з метою організації запитуваної допомоги під час подорожі. Дані, які обробляються на підставі згоди, повинні бути необхідними для надання запитуваної послуги. Крім того, рейси до Будапешта залишаються доступними й без туристичної допомоги. Зверніть увагу, що оскільки ці дані необхідні для надання запитуваної послуги, стаття 7(4) не застосовується.

101. Приклад 20: Успішна компанія спеціалізується на виготовленні на замовлення окулярів для лиж та сноубордів, а також інших видів окулярів для занять спортом на відкритому повітрі. Ідея полягає в тому, що люди можуть носити їх без власних окулярів. Компанія отримує замовлення в центральному пункті й доставляє продукцію з одного місця по всьому ЄС.

102. Для того, щоб мати змогу надавати свої індивідуальні продукти клієнтам, які страждають на короткозорість, цей контролер запитує згоду на використання інформації про стан їхніх очей. Клієнти надають необхідні дані про стан здоров'я, такі як дані про свої рецепти, під час оформлення замовлення в режимі онлайн. Без цього неможливо надати замовлені індивідуальні окуляри. Компанія також пропонує серії окулярів зі стандартизованими значеннями корекції. Клієнти, які не бажають ділитися даними про стан здоров'я, можуть вибрати стандартні версії. Таким чином, необхідна явна згода відповідно до статті 9, і згоду можна вважати вільно наданою.

5 ДОДАТКОВІ УМОВИ ДЛЯ ОТРИМАННЯ ДІЙСНОЇ ЗГОДИ

103. GDPR запроваджує вимоги до контролерів вжити додаткових заходів, щоб забезпечити отримання, збереження та можливість довести дійсну згоду. Стаття 7 GDPR встановлює ці додаткові умови для отримання дійсної згоди, з конкретними положеннями про ведення записів про згоду та право на легке відкликання згоди. Стаття 7 також застосовується до згоди, про яку йдеться в інших статтях GDPR, наприклад, у статтях 8 і 9. Нижче наведено інструкції щодо додаткової вимоги довести дійсну згоду та відкликання згоди.

5.1 Доведення згоди

104. У статті 7(1) GDPR чітко окреслює обов'язок контролера довести згоду суб'єкта даних. Відповідно до статті 7(1), тягар доведення лежить на контролері.

105. У преамбулі 42 зазначено: *«У разі, якщо обробку здійснюють на підставі згоди суб'єкта даних, контролер повинен бути спроможним довести те, що суб'єкт даних надав згоду на операцію з обробки».*

Прийнято

106. Контролери можуть вільно розробляти методи дотримання цього положення таким чином, щоб це відповідало їхній повсякденній діяльності. Водночас обов'язок довести, що контролер отримав дійсну згоду, сам по собі не повинен призводити до надмірних обсягів додаткової обробки даних. Це означає, що контролери повинні мати достатньо даних, щоб показати зв'язок з обробкою (показати, що згоду було отримано), але вони не повинні збирати більше інформації, ніж це необхідно.

107. Контролер повинен довести, що від суб'єкта даних було отримано дійсну згоду. GDPR не визначає, як саме це має бути зроблено. Однак контролер повинен бути в змозі довести, що суб'єкт даних у конкретному випадку надав свою згоду. Поки триває відповідна операція з обробки даних, обов'язок довести згоду продовжує існувати. Після завершення діяльності з обробки підтвердження згоди слід зберігати не довше, ніж це необхідно для дотримання правових зобов'язань або для встановлення, здійснення чи захисту правових претензій, відповідно до статті 17(3)(b) та (e).

108. Наприклад, контролер може вести облік отриманих заяв про надання згоди, щоб показати, як було отримано згоду, коли вона була отримана, а також інформацію, надану суб'єкту даних під час отримання згоди, що має бути очевидною. Контролер також повинен довести, що суб'єкт даних був поінформований, а робочий процес контролера відповідав усім відповідним критеріям отримання дійсної згоди. Обґрунтуванням цього зобов'язання в GDPR є те, що контролери несуть відповідальність за отримання дійсної згоди від суб'єктів даних і за механізми згоди, які вони запровадили. Наприклад, в онлайн-середовищі контролер може зберігати інформацію про сеанс, під час якого було надано згоду, разом із документацією робочого процесу отримання згоди під час сеансу та копією інформації, яка була надана суб'єкту даних під час цього сеансу. Недостатньо буде просто посилатися на правильну конфігурацію відповідного вебсайту.

109. Приклад 21: Лікарня започатковує науково-дослідницьку програму під назвою «Проект X», для якої необхідні стоматологічні картки реальних пацієнтів. Учасників набирають за допомогою телефонних дзвінків пацієнтам, які добровільно погодилися бути у списку кандидатів, до яких можна звернутися з цією метою. Контролер запитує у суб'єктів даних явну згоду на використання їхніх стоматологічних записів. Згода отримується під час телефонної розмови шляхом запису усної заяви суб'єкта даних, у якій суб'єкт даних підтверджує, що він погоджується на використання його даних для цілей проекту X.

110. GDPR не встановлює конкретного терміну дії згоди на обробку даних. Тривалість дії згоди залежить від контексту, обсягу початкової згоди та очікувань суб'єкта даних. Якщо операції з обробки даних значно змінюються або еволюціонують, то початкова згода втрачає чинність. У такому випадку необхідно отримати нову згоду.

111. EDPB рекомендує як найкращу практику оновлювати згоду через відповідні проміжки часу. Повторне надання всієї інформації допомагає гарантувати, що суб'єкт даних залишається добре поінформованим про те, як використовуються його дані та як здійснювати свої права.[51]

[51] Див. настанови Робочої групи за статтею 29 щодо прозорості відповідно до Регламенту 2016/679,РД 260, версія 01 – схвалені EDPB.
Прийнято

5.2 Відкликання згоди

112. Відкликанню згоди відведено важливе місце в GDPR. Положення та згадки про відкликання згоди в GDPR можна розглядати як кодифікацію існуючого тлумачення цього питання у Висновках Робочої групи за статтею 29.[52]

113. Стаття 7(3) GDPR передбачає, що контролер повинен забезпечити можливість відкликання згоди суб'єктом даних так само легко, як і надання згоди, і в будь-який час. GDPR не говорить про те, що надання та відкликання згоди завжди має відбуватися за допомогою однієї і тієї ж дії.

114. Однак, коли згода отримується за допомогою електронних засобів лише одним кліком миші, свайпом або натисканням клавіші, суб'єкти даних повинні на практиці мати можливість так само легко відкликати цю згоду. Якщо згоду отримано за допомогою спеціального користувацького інтерфейсу (наприклад, через вебсайт, додаток, обліковий запис для входу в систему, інтерфейс пристрою Інтернету речей або електронною поштою), безсумнівно, суб'єкт даних повинен мати можливість відкликати згоду через той самий електронний інтерфейс, оскільки перехід на інший інтерфейс з єдиною метою відкликання згоди вимагатиме надмірних зусиль. Крім того, суб'єкт даних повинен мати можливість відкликати свою згоду без шкоди для себе. Це означає, серед іншого, що контролер повинен забезпечити можливість відкликання згоди безкоштовно або без зниження рівня обслуговування.[53]

115. Приклад 22: Музичний фестиваль продає квитки через онлайн-агента з продажу квитків. Під час кожного онлайн-продажу квитків запитується згода на використання контактних даних у маркетингових цілях. Щоб висловити свою згоду на це, клієнти можуть вибрати «Ні» або «Так». Контролер інформує клієнтів про те, що вони мають можливість відкликати свою згоду. Для цього вони можуть безкоштовно звернутися до колл-центру в робочі дні з 8:00 до 17:00. У цьому прикладі контролер не дотримується статті 7(3) GDPR. Відкликання згоди в цьому випадку вимагає телефонного дзвінка в робочий час, що є більш обтяжливим, ніж один клік мишкою, необхідний для надання згоди через онлайн-продавця квитків, який працює 24/7.

[52] Робоча група за статтею 29 обговорила це питання у своєму Висновку щодо надання згоди (див. Висновок 15/2011 про визначення поняття згоди (РД 187), с. 9, 13, 20, 27 і 32-33) і, серед іншого, у своєму Висновку щодо використання даних про місцезнаходження. (див. Висновок 5/2005 про використання даних про місцезнаходження з метою надання послуг з доданою вартістю (РД 115), с. 7).

[53] Див. також Висновок 4/2010 Робочої групи за статтею 29 про Європейський кодекс поведінки FEDMA щодо використання персональних даних у прямому маркетингу (РД 174) та Висновок щодо використання даних про місцезнаходження з метою надання послуг з доданою вартістю (РД 115).

Прийнято

116. Вимога легкого відкликання описана в GDPR як необхідний аспект дійсної згоди. Якщо право на відкликання не відповідає вимогам GDPR, то механізм надання згоди контролером не відповідає положенням GDPR. Як згадувалося в розділі 3.1 про умови надання *інформованої* згоди, контролер повинен повідомити суб'єкта даних про право відкликати згоду до того, як він її фактично надасть, відповідно до статті 7(3) GDPR. Крім того, в рамках зобов'язання щодо забезпечення прозорості контролер повинен інформувати суб'єктів даних про те, як вони можуть реалізувати свої права.[54]

117. За загальним правилом, якщо згоду відкликано, всі операції з обробки даних, які ґрунтувалися на згоді та були здійснені до відкликання згоди — і відповідно до GDPR — залишаються законними, однак контролер повинен зупинити відповідні дії з обробки. Якщо немає іншої законної підстави, що виправдовує обробку (наприклад, подальше зберігання) даних, вони повинні бути видалені контролером.[55]

118. Як уже згадувалося раніше в цих настановах, дуже важливо, щоб контролери оцінювали цілі, для яких фактично обробляються дані, та законні підстави, на яких вони ґрунтуються, до того, як збирати дані. Часто компанії потребують персональних даних для кількох цілей, і обробка ґрунтується на кількох законних підставах, наприклад, дані клієнтів можуть ґрунтуватися на договорі та згоді. Отже, відкликання згоди не означає, що контролер повинен видалити дані, які обробляються з метою, що ґрунтується на виконанні договору із суб'єктом даних. Тому контролери повинні із самого початку чітко розуміти, яка мета застосовується до кожного елемента даних і на яку законну підставу вони покладаються.

119. Контролери зобов'язані видаляти дані, які оброблялися на підставі згоди, як тільки ця згода відкликається, за умови, що немає іншої мети, яка б виправдовувала подальше зберігання.[56] Окрім цієї ситуації, описаної в статті 17(1)(b), окремий суб'єкт даних може вимагати видалення інших даних, що стосуються його, які обробляються на іншій законній підставі, наприклад, на підставі статті 6(1)(b).[57] Контролери зобов'язані оцінити, чи є доцільною подальша обробка таких даних, навіть за відсутності запиту на видалення від суб'єкта даних.[58]

120. У випадках, коли суб'єкт даних відкликає свою згоду, а контролер бажає продовжити обробку персональних даних на іншій законній підставі, він не може мовчки перейти від згоди (яка відкликана) до цієї іншої законної підстави. Будь-яка зміна законної підстави для обробки повинна бути повідомлена суб'єкту даних відповідно до вимог щодо інформації, викладених у статтях 13 і 14, та згідно із загальним принципом прозорості.

---

[54] У преамбулі 39 GDPR, яка посилається на статті 13 і 14 цього Регламенту, зазначено, що *«фізичні особи повинні бути обізнані про те, що їхні персональні дані збирають, використовують, обговорюють або іншим чином обробляють, а також про те, якою мірою обробляють чи будуть обробляти персональні дані».*

[55] Див. статтю 17(1)(b) та (3) GDPR.

[56] У такому випадку інша мета, що виправдовує обробку, повинна мати свою окрему законну підставу. Це не означає, що контролер може замінити згоду на іншу законну підставу, див. розділ 6 нижче.

[57] Див. статтю 17, включаючи винятки, які можуть застосовуватися, та преамбулу 65 GDPR.

[58] Див. також статтю 5(1)(e) GDPR.

Прийнято

6 ВЗАЄМОЗВ'ЯЗОК МІЖ ЗГОДОЮ ТА ІНШИМИ ЗАКОННИМИ ПІДСТАВАМИ ЗА СТАТТЕЮ 6 GDPR

121. Стаття 6 встановлює умови для законної обробки персональних даних та описує шість законних підстав, на які може покладатися контролер. Застосування однієї із цих шести підстав має бути встановлене до початку обробки та у зв'язку з конкретною метою.[59]

122. Тут важливо зазначити, що якщо контролер вирішить покладатися на згоду для будь-якої частини обробки, він повинен бути готовий поважати цей вибір і зупинити цю частину обробки, якщо особа відкликає свою згоду. Повідомлення про те, що дані будуть оброблятися на основі згоди, тоді як насправді покладаються на іншу законну підставу, було б принципово несправедливим щодо фізичних осіб.

123. Іншими словами, контролер не може переходити від згоди до інших законних підстав. Наприклад, не дозволяється ретроспективно використовувати законну підставу для виправдання обробки, якщо виникли проблеми із дійсністю згоди. Через вимогу розкривати законну підставу, на яку покладається контролер під час збору персональних даних, контролери повинні заздалегідь, до початку збору, вирішити, якою є застосовна законна підстава.

7 КОНКРЕТНІ ПРОБЛЕМНІ ПИТАННЯ В GDPR

7.1 Діти (стаття 8)

124. Порівняно із чинною директивою, GDPR створює додатковий рівень захисту в тих випадках, коли обробляються персональні дані вразливих фізичних осіб, особливо дітей. Стаття 8 запроваджує додаткові зобов'язання щодо забезпечення підвищеного рівня захисту даних дітей у зв'язку з послугами інформаційного суспільства. Причини посиленого захисту зазначені в преамбулі 38: *«[...] вони можуть бути менш обізнаними про відповідні ризики, наслідки та гарантії, а також про свої права щодо обробки персональних даних. [...]»*. У преамбулі 38 також зазначено, що *«Такий особливий захист повинен, зокрема, застосовуватися до використання персональних даних дітей для цілей маркетингу або створення профілів особистості чи користувача та збирання персональних даних щодо дітей під час користування послугами, що пропонують безпосередньо дитині».* Слова «зокрема» вказують на те, що конкретний захист не обмежується маркетингом або профайлінгом, а включає більш широке поняття «збір персональних даних щодо дітей».

[59] Відповідно до статей 13(1)(c) та/або 14(1)(c), контролер повинен повідомити про це суб'єкта даних.

125. Стаття 8(1) зазначає, що у випадках, коли згода застосовується у зв'язку з наданням послуг інформаційного суспільства безпосередньо дитині, обробка персональних даних дитини є законною, якщо дитині виповнилося 16 років. Якщо дитина не досягла 16-річного віку, така обробка є законною лише в тому випадку, якщо і тою мірою, в якій згода надана або санкціонована особою, яка несе батьківську відповідальність за дитину.[60] Щодо вікової межі дійсної згоди GDPR забезпечує гнучкість: держави-члени можуть законодавчо встановити нижчий вік, але цей вік не може бути нижчим за 13 років.

126. Як зазначено в розділі 3.1. про інформовану згоду, інформація повинна бути зрозумілою для аудиторії, до якої звертається контролер, приділяючи особливу увагу становищу дітей. Для того, щоб отримати «інформовану згоду» від дитини, контролер повинен пояснити мовою, зрозумілою для дітей, як він має намір обробляти дані, які він збирає.[61] Якщо згоду мають давати батьки, то може знадобитися набір інформації, який дозволить дорослим прийняти поінформоване рішення.

127. З вищевикладеного зрозуміло, що стаття 8 застосовується лише тоді, коли виконуються такі умови:

- Обробка пов'язана з наданням послуг інформаційного суспільства безпосередньо дитині[62].[63]
- Обробка ґрунтується на згоді.

7.1.1 Послуги інформаційного суспільства

128. Для визначення обсягу терміну «послуга інформаційного суспільства» в GDPR у статті 4(25) GDPR робиться посилання на Директиву 2015/1535.

---

[60] Не обмежуючи можливості законодавства держав-членів відступати від вікових обмежень, див. статтю 8(1).

[61] Преамбула 58 GDPR підтверджує це зобов'язання, зазначаючи, що, за необхідності, контролер повинен переконатися, що надана інформація є зрозумілою для дітей.

[62] Відповідно до статті 4(25) GDPR послуга інформаційного суспільства означає послугу, визначену в пункті (b) статті 1(1) Директиви 2015/1535: *«(b) «послуга» означає будь-яку послугу інформаційного суспільства, тобто будь-яку послугу, що зазвичай надається за винагороду, на відстані, за допомогою електронних засобів та за індивідуальним запитом одержувача послуг. Для цілей цього визначення: (i) «на відстані» означає, що послуга надається без одночасної присутності сторін; (ii) «електронними засобами» означає, що послуга спочатку надсилається та отримується в місці призначення за допомогою електронного обладнання для обробки (включаючи цифрове стиснення) та зберігання даних, а також повністю передається та отримується дротовим зв'язком, радіо, оптичними засобами або іншими електромагнітними засобами; (iii) «за індивідуальним запитом отримувача послуг» означає, що послуга надається шляхом передачі даних за індивідуальним запитом».* Орієнтовний перелік послуг, які не підпадають під це визначення, викладено в Додатку I до зазначеної Директиви. Див. також преамбулу 18 Директиви 2000/31.

[63] Відповідно до Конвенції ООН про захист дітей, стаття 1, *«[...] дитина означає кожну людську істоту до досягнення вісімнадцятирічного віку, якщо за законом, що застосовується до дитини, вона не досягає повноліття раніше»*, див. Організація Об'єднаних Націй, Резолюція Генеральної Асамблеї 44/25 від 20 листопада 1989 року (Конвенція про права дитини).
Прийнято

129. Оцінюючи обсяг цього визначення, EDPB також посилається на прецедентне право Суду ЄС.[64] Суд ЄС постановив, що *послуги інформаційного суспільства* охоплюють договори та інші послуги, які укладаються або передаються в режимі онлайн. Якщо послуга складається з двох економічно незалежних компонентів, один з яких є онлайн, наприклад, пропозиція та прийняття пропозиції в контексті укладення договору або інформація, що стосується продуктів або послуг, включаючи маркетингову діяльність, цей компонент визначається як послуга інформаційного суспільства, а інший компонент, що полягає у фізичній доставці або розповсюдженні товарів, не охоплюється поняттям послуги інформаційного суспільства. Надання послуги онлайн підпадає під сферу дії терміну *«послуга інформаційного суспільства»* у статті 8 GDPR.

7.1.2 Надання послуг безпосередньо дитині

130. Включення формулювання «пропонується безпосередньо дитині» вказує на те, що стаття 8 призначена для застосування до деяких, а не до всіх послуг інформаційного суспільства. У зв'язку із цим, якщо постачальник послуг інформаційного суспільства дає зрозуміти потенційним користувачам, що він пропонує свої послуги тільки особам віком від 18 років, і це не спростовується іншими доказами (наприклад, змістом сайту або маркетинговими планами), то послуга не вважатиметься такою, що «пропонується безпосередньо дитині», і стаття 8 не застосовуватиметься.

7.1.3 Вік

131. GDPR визначає, що *«Держави-члени можуть законодавчо встановити нижчий вік для цих цілей за умови, що такий нижчий вік не буде нижчим за 13 років».* Контролер повинен знати про ці різні національні закони, беручи до уваги аудиторію, на яку спрямовані його послуги. Зокрема, слід зазначити, що регулятор, який надає транскордонні послуги, не завжди може покладатися на дотримання лише законодавства держави-члена, у якій він має головний офіс, а повинен дотримуватися відповідних національних законів кожної держави-члена, у якій він пропонує послуги інформаційного суспільства. Це залежить від того, чи вирішить держава-член використовувати місце головного офісу контролера як точку відліку у своєму національному законодавстві, чи місце проживання суб'єкта даних. Держави-члени повинні, перш за все, враховувати найкращі інтереси дитини при прийнятті рішення про вибір. Робоча група закликає держави-члени шукати узгоджене рішення в цьому питанні.

132. Надаючи послуги інформаційного суспільства дітям на основі згоди, контролери повинні докладати необхідних зусиль для перевірки того, що користувач досяг віку цифрової згоди, і ці заходи повинні відповідати характеру та ризикам діяльності з обробки даних.

---

[64] Див. Суд ЄС, 2 грудня 2010 року, справа C-108/09, *(Ker-Optika)*, п. 22 і 28. Стосовно «комплексних послуг» EDPB також посилається на справу C-434/15 *(Asociacion Profesional Elite Taxi v Uber Systems Spain SL)*, п. 40, у якому зазначено, що послуга інформаційного суспільства, яка є невід'ємною частиною загальної послуги, основним компонентом якої не є послуга інформаційного суспільства (у цьому випадку транспортна послуга), не повинна кваліфікуватися як «послуга інформаційного суспільства».
Прийнято

133. Якщо користувачі заявляють, що вони досягли віку цифрової згоди, то контролер може провести відповідні перевірки, щоб переконатися, що ця заява відповідає дійсності. Хоча необхідність докладати обґрунтованих зусиль для перевірки віку прямо не зазначена в GDPR, вона неявно вимагається, оскільки якщо дитина дає згоду, не будучи достатньо дорослою, щоб надати дійсну згоду від свого імені, то це зробить обробку даних незаконною.

134. Якщо користувач заявляє, що він не досяг віку цифрової згоди, контролер може прийняти цю заяву без подальших перевірок, але повинен буде отримати дозвіл батьків і переконатися, що особа, яка надає таку згоду, є носієм батьківської відповідальності.

135. Перевірка віку не повинна призводити до надмірної обробки даних. Механізм, обраний для перевірки віку суб'єкта даних, повинен включати оцінку ризику запропонованої обробки. У деяких ситуаціях з низьким рівнем ризику може бути доцільним вимагати від нового абонента послуги повідомити рік свого народження або заповнити форму про те, що він є (не є) неповнолітнім.[65] Якщо виникають сумніви, контролер повинен переглянути свої механізми перевірки віку в конкретному випадку й розглянути, чи потрібні альтернативні перевірки.[66]

7.1.4 Згода дитини та відповідальність батьків

136. Що стосується повноважень особи, яка несе батьківську відповідальність, GDPR не визначає практичних способів отримання згоди батьків або встановлення того, що будь-яка особа має право здійснювати цю дію.[67] Тому EDPB рекомендує застосовувати обґрунтований підхід відповідно до статті 8(2) GDPR та статті 5(1)(c) GDPR (мінімізація даних). Обґрунтований підхід може полягати в тому, щоб зосередитися на отриманні обмеженого обсягу інформації, наприклад, контактних даних батьків або опікунів.

137. Те, що є обґрунтованим як з точки зору перевірки того, що користувач є достатньо дорослим для надання власної згоди, так і з точки зору перевірки того, що особа, яка надає згоду від імені дитини, є носієм батьківської відповідальності, може залежати від ризиків, притаманних обробці, а також від наявних технологій. У випадках з низьким рівнем ризику може бути достатньо підтвердження батьківської відповідальності через електронну пошту. І навпаки, у випадках високого ризику може бути доцільно запросити більше доказів, щоб контролер міг перевірити та зберегти інформацію відповідно до статті 7(1) GDPR.[68] Довірені сторонні служби перевірки можуть запропонувати рішення, які мінімізують обсяг персональних даних, які контролер повинен обробляти самостійно.

---

[65] Хоча це не може бути універсальним рішенням у всіх випадках, це приклад того, як працювати із цим положенням.

[66] Див. Висновок 5/2009 Робочої групи за статтею 29 щодо послуг соціальних мереж (РД 163).

[67] Робоча група за статтею 29 зазначає, що не завжди особа, яка несе батьківську відповідальність, є рідним батьком (матір'ю) дитини, і що батьківську відповідальність можуть нести кілька сторін, серед яких можуть бути як юридичні, так і фізичні особи.

[68] Наприклад, батьків або опікунів можуть попросити здійснити платіж у розмірі 0,01 євро на користь контролера за допомогою банківської транзакції, включно з коротким підтвердженням у рядку опису транзакції, що власник банківського рахунку є особою, яка несе батьківську відповідальність за користувача. За необхідності, слід передбачити альтернативний метод перевірки, щоб запобігти неправомірному дискримінаційному ставленню до осіб, які не мають банківського рахунку.
Прийнято

138. Приклад 23: Платформа онлайн-ігор хоче переконатися, що неповнолітні клієнти підписуються на її послуги лише за згодою своїх батьків або опікунів. Контролер виконує такі дії:

139. Крок 1: Просить користувача вказати, чи є він молодшим або старшим за 16 років (або альтернативний вік цифрової згоди). Якщо користувач вказує, що він не досяг віку цифрової згоди, це означає, що він не досяг віку, з якого надається цифрова згода:

140. Крок 2: Сервіс інформує дитину про те, що батьки або опікуни повинні надати згоду або дозвіл на обробку, перш ніж послуга буде надана дитині. Користувача просять розкрити адресу електронної пошти батьків або опікуна.

141. Крок 3: Сервіс зв'язується з батьками або опікуном та отримує їхню згоду електронною поштою на обробку та вживає необхідних заходів для підтвердження того, що доросла особа несе батьківську відповідальність.

142. Крок 4: у разі надходження скарг платформа вживає додаткових заходів для перевірки віку підписника.

143. Якщо платформа виконала інші вимоги щодо отримання згоди, вона може відповідати додатковим критеріям статті 8 GDPR, виконавши ці кроки.

144. Цей приклад показує, що контролер може довести, що було докладено необхідних зусиль для забезпечення отримання дійсної згоди щодо послуг, які надаються дитині. Стаття 8(2), зокрема, додає, що «*Контролер має докласти необхідних зусиль для перевірки того, що згода надана або уповноважена особою, яка несе батьківську відповідальність за дитину, беручи до уваги наявні технології*».

145. Саме контролер повинен визначити, які заходи є доцільними в кожному конкретному випадку. Як правило, контролери повинні уникати рішень щодо перевірки, які самі по собі передбачають надмірний збір персональних даних.

146. EDPB визнає, що можуть бути випадки, коли перевірка є складною (наприклад, коли діти, які надають власну згоду, ще не встановили «ідентифікаційний слід», або коли відповідальність батьків нелегко перевірити). Це може бути враховано при прийнятті рішення про те, які зусилля є обґрунтованими, але від контролерів також очікується, що вони будуть постійно переглядати свої процедури та доступні технології.

147. Що стосується автономії суб'єкта даних щодо надання згоди на обробку своїх персональних даних та повного контролю над обробкою, згода особи, яка несе батьківську відповідальність або уповноваженої особою, яка несе батьківську відповідальність, на обробку персональних даних дітей може бути підтверджена, змінена або відкликана, як тільки суб'єкт даних досягне віку, з якого надається цифрова згода.

148. На практиці це означає, що якщо дитина не вчиняє жодних дій, згода, надана особою, яка несе батьківську відповідальність або уповноваженою особою, яка несе батьківську відповідальність, на обробку персональних даних, надана до досягнення віку цифрової згоди, залишатиметься дійсною підставою для обробки.

Прийнято

149. Після досягнення віку цифрової згоди дитина матиме можливість самостійно відкликати свою згоду відповідно до статті 7(3). Відповідно до принципів справедливості та підзвітності, контролер повинен повідомити дитину про цю можливість.[69]

150. Важливо зазначити, що відповідно до преамбули 38, згода батьків або опікунів не потрібна в контексті профілактичних або консультативних послуг, що пропонуються безпосередньо дитині. Наприклад, надання послуг із захисту дітей, що пропонуються дитині в Інтернеті за допомогою онлайн-чату, не вимагає попереднього дозволу батьків.

151. Зрештою, GDPR зазначає, що правила, які стосуються вимог щодо батьківського дозволу стосовно неповнолітніх, не повинні втручатися в «загальне договірне право держав-членів, таке як правила щодо дійсності, укладення або дії договору стосовно дитини». Таким чином, вимоги щодо дійсної згоди на використання даних про дітей є частиною нормативно-правової бази, яку слід розглядати окремо від національного договірного права. Крім того, у цих настановах не розглядається питання, чи є законним укладення неповнолітніми договорів в Інтернеті. Обидва правові режими можуть застосовуватися одночасно, і сфера дії GDPR не включає гармонізацію національних положень договірного права.

152.

7.2 Наукові дослідження

153. Визначення цілей наукових досліджень має суттєві наслідки для спектра діяльності з обробки даних, яку може здійснювати контролер. Термін *«наукові дослідження»* не визначений у GDPR. У преамбулі 159 зазначено «(...) *У рамках цього Регламенту, обробку персональних даних для цілей наукового дослідження необхідно тлумачити в широкому сенсі.* (...)», однак EDPB вважає, що це поняття не може виходити за межі його загального значення, і розуміє, що *«наукове дослідження»* в цьому контексті означає дослідницький проект, створений відповідно до відповідних галузевих методологічних та етичних стандартів, згідно з належною практикою.

[69] Крім того, суб'єкти даних повинні знати про своє право на забуття (право бути забутим), викладене в статті 17, яке особливо стосується згоди, наданої, коли суб'єкт даних був ще дитиною (див. преамбулу 63).
Прийнято

154. Коли згода є законною підставою для проведення досліджень відповідно до GDPR, цю згоду на використання персональних даних слід відрізняти від інших вимог щодо надання згоди, які слугують етичним стандартом або процедурним зобов'язанням. Приклад такого процедурного зобов'язання, коли обробка ґрунтується не на згоді, а на іншій законній підставі, можна знайти в Регламенті клінічних випробувань. У контексті законодавства про захист даних останню форму надання згоди можна розглядати як додаткову гарантію. [70] Водночас GDPR не обмежує застосування статті 6 лише згодою щодо обробки даних для дослідницьких цілей. Якщо існують відповідні гарантії, такі як вимоги статті 89(1), а обробка є справедливою, законною, прозорою і відповідає стандартам мінімізації даних та індивідуальним правам, можуть бути доступні інші законні підстави, такі як стаття 6(1)(e) або (f).[71] Це також стосується спеціальних категорій даних відповідно до відступу від статті 9(2)(j).[72]

155. Преамбула 33, як видається, вносить певну гнучкість у ступінь конкретизації та деталізації згоди в контексті наукових досліджень. У преамбулі 33 зазначено: *«Часто неможливо повністю визначити мету обробки персональних даних для цілей наукових досліджень під час збору даних. Тому суб'єкти даних повинні мати можливість надавати свою згоду на певні напрямки наукових досліджень, якщо це відповідає визнаним етичним стандартам наукових досліджень. Суб'єкти даних повинні мати можливість надавати свою згоду лише на певні напрямки досліджень або частини дослідницьких проектів в обсязі, дозволеному поставленою метою».*

156. По-перше, слід зазначити, що преамбула 33 не скасовує зобов'язання щодо вимоги конкретної згоди. Це означає, що, в цілому, науково-дослідні проекти можуть включати персональні дані на основі згоди лише в тому випадку, якщо вони мають чітко визначену мету. Для випадків, коли цілі обробки даних у рамках науково-дослідного проекту не можуть бути визначені із самого початку, преамбула 33 допускає, як виняток, що мета може бути описана на більш загальному рівні.

157. Враховуючи суворі умови, встановлені статтею 9 GDPR щодо обробки спеціальних категорій даних, EDPB зазначає, що коли спеціальні категорії даних обробляються на основі явної згоди, застосування гнучкого підходу преамбули 33 підлягатиме більш суворому тлумаченню та вимагає високого ступеня ретельної перевірки.

158. Якщо розглядати GDPR у цілому, то його не можна тлумачити так, щоб дозволити контролеру обійти ключовий принцип визначення цілей, для яких запитується згода суб'єкта даних.

---

[70] Див. також преамбулу 161 GDPR.

[71] Стаття 6(1)(c) може також застосовуватися до частин операцій з обробки, які окремо вимагаються законом, таких як збір надійних і достовірних даних відповідно до протоколу, затвердженого державою-членом відповідно до Регламенту клінічних випробувань.

[72] Окремі випробування лікарських засобів можуть проводитися на основі законодавства ЄС або національного законодавства відповідно до статті 9(2)(i).

Прийнято

159. Якщо цілі дослідження не можуть бути повністю визначені, контролер повинен шукати інші способи забезпечити найкраще виконання вимог щодо надання згоди, наприклад, дозволити суб'єктам даних давати згоду на дослідження в більш загальних термінах і для конкретних етапів дослідницького проекту, про які вже відомо, що вони відбуватимуться на самому початку. У міру просування дослідження згода на наступні етапи проекту може бути отримана до того, як почнеться наступний етап. Проте, така згода повинна відповідати етичним стандартам наукових досліджень.

160. Крім того, у таких випадках контролер може застосовувати додаткові захисні заходи. Наприклад, стаття 89(1) підкреслює необхідність захисних заходів при обробці даних для наукових, історичних або статистичних цілей. Ці цілі *«підлягають відповідним гарантіям, згідно із цим регламентом, для захисту прав і свобод суб'єктів даних».* Мінімізація даних, знеособлення та безпека даних згадуються як можливі гарантії.[73] Знеособлення є кращим рішенням, якщо мета дослідження може бути досягнута без обробки персональних даних.

161. Прозорість є додатковим запобіжником, коли обставини дослідження не дозволяють отримати конкретну згоду. Відсутність конкретизації мети може бути компенсована інформацією про розвиток мети, яка регулярно надається контролерами в міру просування дослідницького проекту, так що з часом згода буде максимально конкретною. Таким чином, суб'єкт даних має принаймні базове розуміння ситуації, що дозволяє йому оцінити, чи варто використовувати, наприклад, право на відкликання згоди згідно зі статтею 7(3).[74]

162. Крім того, наявність комплексного плану дослідження, доступного для ознайомлення суб'єктами даних до того, як вони дадуть згоду, може допомогти компенсувати відсутність конкретизації мети. [75] План дослідження повинен якомога чіткіше визначати питання дослідження та передбачені методи роботи. План дослідження також може сприяти дотриманню статті 7(1), оскільки контролери повинні показати, яка інформація була доступна суб'єктам даних на момент надання згоди, щоб мати можливість довести, що згода є дійсною.

---

[73] Див. наприклад, преамбулу 156. Обробка персональних даних для наукових цілей має також відповідати іншим відповідним законодавчим актам, наприклад, про клінічні випробування, див. преамбулу 156, де згадується Регламент (ЄС) № 536/2014 Європейського Парламенту та Ради від 16 квітня 2014 року про клінічні випробування лікарських засобів для людини. Див. також Висновок 15/2011 Робочої групи за статтею 29 щодо визначення поняття згоди (РД 187), с. 7: *«Крім того, отримання згоди не скасовує зобов'язань контролера відповідно до статті 6 щодо справедливості, необхідності та обґрунтованості, а також якості даних. Наприклад, навіть якщо обробка персональних даних ґрунтується на згоді користувача, це не легітимізує збір даних, які є надмірними щодо конкретної мети». [...] Загалом, згоду слід розглядати не як виняток з інших принципів захисту даних, а як гарантію. Це насамперед підстава для законності, і вона не скасовує застосування інших принципів».*

[74] Інші заходи прозорості також можуть бути доцільними. Коли контролери беруть участь в обробці даних для наукових цілей, хоча повна інформація не може бути надана на початковому етапі, вони можуть призначити конкретну контактну особу, до якої суб'єкти даних можуть звертатися з питаннями.

[75] Таку можливість можна знайти в статті 14(1) чинного Закону Фінляндії про захист персональних даних (*Henkilötietolaki*, 523/1999).

Прийнято

163. Важливо нагадати, що у випадках, де згода використовується як законна підстава для обробки, суб'єкт даних повинен мати можливість відкликати свою згоду. EDPB зазначає, що відкликання згоди може зашкодити науковим дослідженням, які потребують даних, що можуть бути пов'язані з особами, однак GDPR чітко визначає, що згоду можна відкликати, і контролери повинні діяти відповідно до цього — для наукових досліджень не існує винятку із цієї вимоги. Якщо контролер отримує запит на відкликання, він, у цілому, повинен негайно видалити персональні дані, якщо він бажає продовжувати використовувати дані для цілей дослідження.[76]

7.3 Права суб'єкта даних

164. Якщо діяльність з обробки даних ґрунтується на згоді суб'єкта даних, це впливає на його права. Суб'єкти даних можуть мати право на перенесення даних (стаття 20), коли обробка ґрунтується на згоді. Водночас право на заперечення (стаття 21) не застосовується, коли обробка ґрунтується на згоді, хоча право на відкликання згоди в будь-який час може забезпечити подібний результат.

165. У статтях 16-20 GDPR зазначено, що (якщо обробка даних ґрунтується на згоді) суб'єкти даних мають право на видалення даних у разі відкликання згоди, а також право на обмеження, виправлення та доступ до них.[77]

8 ЗГОДА ОТРИМАНА ВІДПОВІДНО ДО ДИРЕКТИВИ 95/46/ЄС

166. Контролери, які наразі обробляють дані на основі згоди відповідно до національного законодавства про захист даних, не зобов'язані автоматично повністю оновлювати всі існуючі відносини із суб'єктами даних у зв'язку з підготовкою до GDPR. Згода, яка була отримана на сьогоднішній день, продовжує залишатися дійсною тою мірою, в якій вона відповідає умовам, викладеним у GDPR.

167. Важливо, щоб контролери детально переглянули поточні робочі процеси та записи до 25 травня 2018 року, щоб переконатися, що наявні згоди відповідають стандарту GDPR (див. преамбулу 171 GDPR[78]). На практиці GDPR піднімає планку щодо впровадження механізмів надання згоди та запроваджує кілька нових вимог, які вимагають від контролерів змінити механізми надання згоди, а не просто переписати політику конфіденційності.[79]

---

[76] Див. також Висновок 05/2014 Робочої групи за статтею 29 про «Методи знеособлення» (РД 216).

[77] У випадках, коли певні види діяльності з обробки даних обмежені відповідно до статті 18 GDPR, для зняття обмежень може знадобитися згода суб'єкта даних.

[78] У преамбулі 171 GDPR зазначено: *«Директива 95/46/ЄС має бути скасована цим Регламентом. Обробка, яка вже здійснюється на дату застосування цього Регламенту, має бути приведена у відповідність до цього Регламенту протягом двох років після набуття чинності цим Регламентом. Якщо обробка ґрунтується на згоді відповідно до Директиви 95/46/ЄС, суб'єкту даних не потрібно повторно надавати свою згоду, якщо спосіб, у який було надано згоду, відповідає умовам цього Регламенту, щоб дозволити контролеру продовжувати таку обробку після дати застосування цього Регламенту. Рішення Комісії та дозволи наглядових органів, прийняті на підставі Директиви 95/46/ЄС, залишаються чинними до їх зміни, заміни або скасування».*

[79] Як зазначено у вступі, GDPR надає подальші роз'яснення та уточнення вимог щодо отримання та доведення дійсної згоди. Багато нових вимог ґрунтуються на Висновку 15/2011 про надання згоди.

168. Наприклад, оскільки GDPR вимагає, щоб контролер мав можливість довести, що було отримано дійсну згоду, всі передбачувані згоди, на які немає посилань, автоматично будуть нижче стандарту згоди GDPR, і їх потрібно буде поновити. Подібно до того, як GDPR вимагає «заяви або чіткої ствердної дії», усі передбачувані згоди, які ґрунтуються на більш неявній формі дії суб'єкта даних (наприклад, попередньо відмічений прапорець «згоден»), також не відповідатимуть стандарту згоди GDPR.

169. Крім того, для того, щоб мати можливість довести, що згоду було отримано, або для того, щоб дозволити більш детальні вказівки на побажання суб'єкта даних, операції та IT-системи, можливо, потребуватимуть перегляду. Також повинні бути доступні механізми, які дозволять суб'єктам даних легко відкликати свою згоду, а також інформація про те, як це зробити. Якщо існуючі процедури отримання та управління згодою не відповідають стандартам GDPR, контролерам необхідно буде отримати нову згоду, що відповідає вимогам GDPR.

170. З іншого боку, оскільки не всі елементи, перелічені в статтях 13 і 14, повинні завжди бути присутніми як умова для отримання інформованої згоди, розширені зобов'язання щодо інформування відповідно до GDPR не обов'язково суперечать безперервності згоди, наданої до набрання чинності GDPR (див. стор. 15 вище). Відповідно до Директиви 95/46/ЄС, не було вимоги інформувати суб'єктів даних про підстави, на яких здійснюється обробка.

171. Якщо контролер виявляє, що згода, отримана раніше за старим законодавством, не відповідає стандартам згоди GDPR, він повинен вжити заходів для дотримання цих стандартів, наприклад, оновити згоду у спосіб, що відповідає GDPR. Відповідно до GDPR, неможливо замінити одну законну підставу на іншу. Якщо контролер не може поновити згоду у відповідний спосіб, а також не може — як разова ситуація — здійснити перехід на відповідність GDPR, ґрунтуючи обробку даних на іншій законній основі, забезпечуючи при цьому справедливість та підзвітність подальшої обробки, діяльність з обробки даних повинна бути зупинена. У будь-якому випадку, контролер повинен дотримуватися принципів законної, справедливої та прозорої обробки.

Прийнято