Настанови

Настанови 01/2022 про права суб’єктів даних — Право на доступ

Версія 2.1

Прийнято 28 березня 2023 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 1.0	18 січня 2022 року	Прийняття Настанов для публічних консультацій
Версія 2.0	28 березня 2023 року	Прийняття Настанов після публічних консультацій
Версія 2.1	30 травня 2024 року	Незначні виправлення

Прийнято

КОРОТКИЙ ОГЛЯД

Право суб'єктів даних на доступ закріплено в статті 8 Хартії основоположних прав ЄС. Вона була частиною європейської нормативно-правової бази захисту даних із самого початку її створення і зараз розвивається більш конкретними та точними правилами в статті 15 GDPR.

Мета та загальна структура права на доступ

Загальною метою права на доступ є надання особам достатньої, прозорої та доступної інформації про обробку їхніх персональних даних, щоб вони могли знати та перевіряти законність обробки й точність оброблених даних. Це полегшить — але не є обов'язковою умовою — здійснення особою інших прав, таких як право на видалення або виправлення.

Право на доступ відповідно до закону про захист даних слід відрізняти від аналогічних прав з іншими цілями, наприклад, права на доступ до державних документів, яке має на меті гарантувати прозорість у прийнятті рішень органами державної влади та належну адміністративну практику.

Однак суб'єкт даних не зобов'язаний пояснювати причини запиту на отримання доступу, і контролер не зобов'язаний аналізувати, чи дійсно запит допоможе суб'єкту даних перевірити законність відповідної обробки або реалізувати інші права. Контролер повинен буде розглянути запит, якщо тільки не буде зрозуміло, що запит подано відповідно до інших правил, ніж правила захисту даних.

Право на доступ включає три різні компоненти:

- підтвердження того, чи обробляються дані про особу;
- доступ до цих персональних даних; та
- доступ до інформації про обробку, зокрема про мету, категорії даних та одержувачів, тривалість обробки, права суб'єктів даних та відповідні гарантії у разі передачі даних до третіх країн.

Загальні міркування щодо оцінки запиту суб'єкта даних

Аналізуючи зміст запиту, контролер повинен оцінити, чи стосується запит персональних даних особи, яка подає запит, чи підпадає запит під дію статті 15, а також чи існують інші, більш конкретні положення, що регулюють доступ до даних у певному секторі. Він також повинен оцінити, чи стосується запит усіх або лише частини оброблених даних про суб'єкта даних.

Конкретних вимог до формату запиту не існує. Контролер повинен забезпечити відповідні та зручні для користувача канали зв'язку, які можуть легко використовуватися суб'єктом даних. Однак суб'єкт даних не зобов'язаний користуватися цими конкретними каналами й може замість цього надіслати запит на офіційну контактну особу контролера. Контролер не зобов'язаний відповідати на запити, надіслані на абсолютно випадкові або явно неправильні адреси.

Якщо контролер не може ідентифікувати дані, які стосуються суб'єкта даних, він повинен повідомити про це суб'єкта даних і може відмовити в доступі, якщо суб'єкт даних не надасть додаткову інформацію, яка дозволить його ідентифікувати. Крім того, якщо контролер має сумніви щодо того, чи є суб'єкт даних тим, за кого він себе видає, він може запросити додаткову

інформацію для підтвердження особи суб'єкта даних. Запит на додаткову інформацію має бути обґрунтованим типу оброблених даних, шкоді, яка може бути заподіяна тощо, щоб уникнути надмірного збору даних.

Обсяг права на доступ

Обсяг права на доступ визначається обсягом поняття персональних даних, як це визначено в статті 4(1) GDPR. Окрім основних персональних даних, таких як ім'я, адреса, номер телефону тощо, під це визначення може підпадати широкий спектр даних, таких як медичні висновки, історія покупок, показники кредитоспроможності, журнали активності, пошукова діяльність тощо. Персональні дані, які пройшли псевдонімізацію, все ще залишаються персональними даними, на відміну від знеособлених даних. Право на доступ стосується персональних даних, що стосуються особи, яка подає запит. Це не повинно тлумачитися надто обмежувально і може включати дані, які можуть стосуватися й інших осіб, наприклад, історію спілкування, що включає вхідні та вихідні повідомлення.

Окрім надання доступу до персональних даних, контролер повинен надати додаткову інформацію про обробку та права суб'єктів даних. Така інформація може ґрунтуватися на тому, що вже міститься в записі контролера про діяльність з обробки (стаття 30 GDPR) та в повідомленні про конфіденційність (статті 13 і 14 GDPR). Однак цю загальну інформацію може знадобитися оновити до моменту подання запиту або адаптувати до операцій з обробки, які здійснюються стосовно конкретної особи, що подає запит.

Як надати доступ

Способи надання доступу можуть відрізнятися залежно від обсягу даних та складності обробки, що здійснюється. Якщо прямо не зазначено інше, запит слід розуміти як такий, що стосується *всіх* персональних даних суб'єкта даних, і контролер може попросити суб'єкта даних конкретизувати запит, якщо він обробляє велику кількість даних.

Контролер повинен буде шукати персональні дані в усіх IT-системах і не IT-системах зберігання даних на основі критеріїв пошуку, які відображають спосіб структурування інформації, наприклад, ім'я та номер клієнта. Передача даних та іншої інформації про обробку повинна здійснюватися у стислій, прозорій, зрозумілій та доступній формі, з використанням чіткої та простої мови. Більш точні вимоги в цьому відношенні залежать від обставин обробки даних, а також від здатності суб'єкта даних сприймати й розуміти повідомлення (наприклад, з урахуванням того, що суб'єкт даних є дитиною або особою з особливими потребами). Якщо дані складаються з кодів або інших «необроблених даних», їх може знадобитися пояснити, щоб вони мали сенс для суб'єкта даних.

Основним способом надання доступу є надання суб'єкту даних копії його даних, але можна передбачити й інші способи (наприклад, усне інформування та доступ на місці), якщо суб'єкт даних про це попросить. Дані можуть бути надіслані електронною поштою, за умови застосування всіх необхідних запобіжних заходів з урахуванням, зокрема характеру даних, або в інший спосіб, наприклад, за допомогою інструменту самообслуговування.

Іноді, коли є велика кількість даних, і суб'єкту даних буде важко зрозуміти інформацію, якщо її надати в одному масиві — особливо в онлайн-контексті — найбільш прийнятним заходом може бути багаторівневий підхід. Надання інформації в різних шарах може полегшити розуміння даних

суб'єктом даних. Контролер повинен бути в змозі довести, що багаторівневий підхід має додаткову цінність для суб'єкта даних, і всі рівні повинні надаватися одночасно, якщо суб'єкт даних обирає такий підхід.

Копія даних і додаткова інформація повинні надаватися в постійній формі, наприклад, у вигляді письмового тексту, який може бути складений у загальноприйнятій електронній формі, щоб суб'єкт даних міг легко їх завантажити. Дані можуть бути надані у вигляді стенограми або компіляції, якщо до них включена вся інформація, і це не змінює або не спотворює зміст інформації.

Запит має бути виконаний якнайшвидше, але в будь-якому випадку протягом одного місяця з моменту отримання запиту. Цей термін може бути продовжений ще на два місяці, якщо це необхідно, з урахуванням складності та кількості запиту. Суб'єкт даних повинен бути поінформований про причину затримки. Контролер повинен вжити необхідних заходів для якнайшвидшої обробки запитів та адаптувати ці заходи до обставин обробки. Якщо дані зберігаються лише протягом дуже короткого періоду часу, повинні бути вжиті заходи, які гарантують, що запит на отримання доступу може бути задоволений без видалення даних під час розгляду запиту. Якщо обробляється велика кількість даних, контролер повинен запровадити процедури та механізми, адаптовані до складності обробки.

Оцінка запиту повинна відображати ситуацію на момент отримання запиту контролером. Навіть ті дані, які можуть бути неправильними або незаконно обробленими, повинні бути надані. Не можна надавати дані, які вже були видалені, наприклад, відповідно до політики зберігання, і тому більше не доступні контролеру.

Ліміти та обмеження

GDPR допускає певні обмеження права на доступ до даних. Жодних інших винятків чи відступів не передбачено. Право на доступ не містить жодних загальних застережень щодо обґрунтованості зусиль, яких має докласти контролер, щоб задовольнити запит суб'єкта даних.

Відповідно до статті 15(4) право на отримання копії не повинно негативно впливати на права й свободи інших осіб. Європейська рада із захисту даних (далі — «EDPB») вважає, що ці права повинні враховуватися не лише при наданні доступу шляхом надання копії, але також, якщо доступ до даних надається іншими способами (наприклад, доступ на місці). Однак стаття 15(4) не застосовується до додаткової інформації про обробку, як зазначено в статті 15(1), підпункти a)-h). Контролер повинен бути в змозі довести, що в конкретній ситуації це може негативно вплинути на права чи свободи інших осіб. Застосування статті 15(4) не повинно призводити до повної відмови у задоволенні запиту суб'єкта даних; це може призвести лише до пропуску або нерозбірливості тих частин, які можуть мати негативні наслідки для прав і свобод інших осіб.

Стаття 12(5) GDPR дозволяє контролерам відхиляти запити, які є явно необґрунтованими або надмірними, або стягувати обґрунтовану плату за такі запити. Ці поняття слід трактувати обмежено. Оскільки існує дуже мало передумов щодо запитів на отримання доступу, сфера розгляду запиту як явно необґрунтованого є досить обмеженою. Надмірність запитів залежить від специфіки сектору, в якому працює контролер. Чим частіше відбуваються зміни в базі даних контролера, тим частіше суб'єкту даних може бути дозволено запитувати доступ до даних, не вважаючи його надмірним. Замість того, щоб відмовити в доступі, контролер може вирішити

стягнути плату із суб'єкта даних. Це буде доцільним лише у випадку надмірних запитів, щоб покрити адміністративні витрати, які такі запити можуть спричинити. Контролер повинен мати можливість довести явно необґрунтований або надмірний характер запиту.

Обмеження права на доступ можуть також існувати в національному законодавстві держав-членів відповідно до статті 23 GDPR та відступів від неї. Контролери, які мають намір покладатися на такі обмеження, повинні ретельно перевірити вимоги національних положень і взяти до уваги будь-які конкретні умови, які можуть застосовуватися. Такі умови можуть полягати в тому, що право на доступ відкладається лише тимчасово або що обмеження стосується лише певних категорій даних.

Зміст

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,

Під час підготовки цих настанов було зібрано інформацію від зацікавлених сторін як у письмовій формі, так і під час спеціального заходу, присвяченого правам суб'єктів даних, з метою виявлення проблем та питань інтерпретації, з якими стикаються при застосуванні відповідних положень GDPR;

ПРИЙНЯЛА ТАКІ НАСТАНОВИ

1 ВСТУП — ЗАГАЛЬНІ ЗАУВАЖЕННЯ

1. У сучасному суспільстві персональні дані обробляються державними та приватними суб'єктами, під час багатьох видів діяльності, для широкого кола цілей та у багато різних способів. Фізичні особи часто можуть перебувати в невигідному становищі з точки зору розуміння того, як обробляються їхні персональні дані, включаючи технологію, що використовується в конкретному випадку, незалежно від того, чи це приватний, чи державний суб'єкт. З метою захисту персональних даних фізичних осіб у таких ситуаціях GDPR передбачено узгоджену та надійну нормативно-правову базу, яка загалом застосовується до різних типів обробки, включаючи конкретні положення, що стосуються прав суб'єктів даних.

2. Право на доступ до персональних даних є одним із прав суб'єктів даних, передбачених главою III GDPR, серед інших прав, таких як, наприклад, право на виправлення та видалення, право на обмеження обробки, право на перенесення, право на заперечення або право не бути об'єктом автоматизованого прийняття індивідуальних рішень, включаючи профайлінг[2]. Право суб'єкта даних на доступ закріплено як у Хартії основоположних прав ЄС (далі — «Хартія»)[3], так і в статті 15

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

[2] Статті 15-22 GDPR.

[3] Відповідно до пункту 1 статті 8 Хартії основоположних прав Європейського Союзу кожен має право на захист своїх персональних даних. Відповідно до речення 2 пункту 2 статті 8 кожен має право на доступ до даних, які були зібрані про нього/неї, та право на їх виправлення.

GDPR, де воно точно сформульоване як право на доступ до персональних даних та іншої пов'язаної з ними інформації.

3. Відповідно до GDPR, право на доступ складається з трьох компонентів: підтвердження того, що персональні дані обробляються, доступ до них та інформація про саму обробку. Суб'єкт даних також може отримати копію оброблених персональних даних, тоді як ця можливість є не додатковим правом суб'єкта даних, а способом забезпечення доступу до даних. Таким чином, право на доступ можна розуміти як можливість суб'єкта даних запитати контролера, чи обробляються його персональні дані, так і як можливість отримати доступ до цих даних та перевірити їх. Контролер зобов'язаний надати суб'єкту даних на його запит інформацію, що підпадає під дію статті 15(1) та (2) GDPR.

4. Реалізація права на доступ здійснюється як у рамках законодавства про захист даних, відповідно до цілей законодавства про захист даних, так і, зокрема, в рамках *«основоположних прав і свобод фізичних осіб і, зокрема, їхнього права на захист персональних даних»*, як зазначено в статті 1(2) GDPR. Право на доступ є важливим аспектом всієї системи захисту даних.

5. Практична мета надання права на доступ полягає в тому, щоб дозволити фізичним особам контролювати свої персональні дані[4]. Для того, щоб ефективно реалізувати цю мету на практиці, GDPR має на меті полегшити цю реалізацію за допомогою низки гарантій, що дозволяють суб'єкту даних здійснювати це право легко, без зайвих обмежень, через обґрунтовані проміжки часу та без надмірних затримок чи витрат. Усе це має призвести до більш ефективного забезпечення права суб'єктів даних на доступ в епоху цифрових технологій, частиною якого в більш широкому сенсі є також право суб'єкта даних подавати скарги до наглядового органу та право на ефективний судовий захист[5].

6. Що стосується розвитку права на доступ як частини нормативно-правової бази захисту даних, слід підкреслити, що воно було аспектом європейської системи захисту даних із самого початку її створення. Порівняно з Директивою 95/46/ЄС, стандарт прав суб'єктів даних, викладений у GDPR, був вдосконалений і посилений; це стосується і права на доступ. Оскільки форми реалізації права на доступ тепер більш точно визначені в GDPR, це право також є більш повчальним з точки зору правової визначеності як для суб'єкта даних, так і для контролера. Крім того, конкретне формулювання статті 15 і точний термін надання даних відповідно до статті 12(3) GDPR, зобов'язує контролера бути готовим до запитів суб'єктів даних, розробивши процедури обробки запитів.

7. Право на доступ не слід розглядати ізольовано, оскільки воно тісно пов'язане з іншими положеннями GDPR, зокрема з принципами захисту даних, включаючи справедливість і законність обробки, зобов'язання контролера щодо прозорості, а також з іншими правами суб'єктів даних, передбаченими у главі III GDPR.

8. У рамках прав суб'єктів даних також важливо підкреслити важливість статті 12 GDPR, яка встановлює вимоги до відповідних заходів, що вживаються контролером при наданні

---

[4] Див. преамбули 7, 68, 75 та 85 GDPR

[5] Див. главу VIII, статті 77, 78 і 79 GDPR

інформації, зазначеної у статтях 13 та 14 GDPR, та повідомлень, зазначених у статтях 15-22 та 34 GDPR; ці вимоги, як правило, визначають форму, спосіб та строки надання відповідей суб'єкту даних, зокрема, для будь-якої інформації, адресованої дитині.

9. EDPB вважає за необхідне надати більш точні вказівки щодо того, як право на доступ має бути реалізоване в різних ситуаціях. Ці настанови спрямовані на аналіз різних аспектів права на доступ до інформації. Зокрема, цей розділ має на меті надати загальний огляд та пояснення змісту самої статті 15, тоді як наступні розділи містять більш глибокий аналіз найбільш поширених практичних питань і проблем, пов'язаних із реалізацією права на доступ до інформації.

2 МЕТА НАДАННЯ ПРАВА НА ДОСТУП, СТРУКТУРА СТАТТІ 15 GDPR ТА ЗАГАЛЬНІ ПРИНЦИПИ

2.1 Мета надання права на доступ

10. Таким чином, право на доступ призначене для того, щоб дозволити фізичним особам контролювати персональні дані, які їх стосуються, оскільки воно дозволяє їм *«знати про законність обробки та перевіряти її»*[6]. Більш конкретно, мета отримання права на доступ полягає в тому, щоб дати можливість суб'єктам даних зрозуміти, як обробляються їхні персональні дані, а також наслідки такої обробки, і перевірити точність оброблених даних без необхідності обґрунтовувати свої наміри. Іншими словами, метою отримання права на доступ є надання особам достатньої, прозорої та доступної інформації про обробку даних, незалежно від використовуваних технологій, а також надання їм можливості перевіряти різні аспекти конкретної діяльності з обробки відповідно до GDPR (наприклад, законність, точність).

11. Тлумачення GDPR, наведене в цих настановах, ґрунтується на прецедентному праві Суду ЄС, яке було винесено до цього часу. Беручи до уваги важливість отримання права на доступ, можна очікувати, що в майбутньому відповідна судова практика зазнає значних змін.

12. Відповідно до рішень Суду ЄС[7], право на доступ слугує цілям гарантування захисту права суб'єктів даних на недоторканність приватного життя та захист даних у зв'язку з обробкою даних, що їх стосуються[8], і може сприяти здійсненню їхніх прав, що випливають, наприклад, зі статей 16-19, 21-22 та 82 GDPR. Однак здійснення права на доступ є правом особи та не залежить від здійснення інших прав, а здійснення інших прав не залежить від здійснення права на доступ.

13. З огляду на широку мету права на доступ, мета надання права на доступ не може бути проаналізована як передумова для здійснення права на доступ контролером у рамках оцінки запитів на отримання доступу. Таким чином, контролери не повинні оцінювати «чому» суб'єкт даних запитує доступ, а лише «що» суб'єкт даних запитує (див. розділ 3 про аналіз запиту) і чи

[6] Преамбула 63 GDPR.

[7] Суд ЄС, справа C-434/16 «Новак», та об'єднані справи C-141/12 та C-372/12, YS та інші.

[8] Суд ЄС, C-434/16 «Новак», п. 56.

зберігаються у них персональні дані, що стосуються цієї особи (див. розділ 4). Тому, наприклад, контролер не повинен відмовляти в доступі на підставі або підозри, що запитувані дані можуть бути використані суб'єктом даних для захисту в суді в разі порушення проти нього кримінальної справи.[9] Щодо лімітів та обмежень права на доступ, будь ласка, див. розділ 6.

Приклад 1: Роботодавець звільнив особу. Через тиждень особа вирішує зібрати докази, щоб подати позов проти колишнього роботодавця за несправедливе звільнення. З цією метою особа звертається до колишнього роботодавця із запитом на отримання доступу до всіх персональних даних, що стосуються її як суб'єкта персональних даних, які обробляє колишній роботодавець як контролер.

Контролер не повинен оцінювати наміри суб'єкта даних, а суб'єкт даних не зобов'язаний повідомляти контролеру причину запиту. Тому, якщо запит відповідає всім іншим вимогам (див. розділ 3), контролер повинен задовольнити запит, якщо тільки запит не виявиться явно необґрунтованим або надмірним відповідно до статті 12 (5) GDPR (див. розділ 6.3), що контролер зобов'язаний довести.

Варіант: Суб'єкт даних користується правом на доступ до персональних даних, що стосуються його або її, під час судового процесу. Однак національне законодавство держави-члена, яке регулює трудові відносини між контролером і суб'єктом даних, містить певні положення, які обмежують обсяг інформації, що підлягає наданню або обміну між сторонами поточних або майбутніх судових процесів, які застосовуються до позову про несправедливе звільнення, поданого суб'єктом даних. У цьому контексті та за умови, що ці національні положення відповідають вимогам, встановленим статтею 23 GDPR[10], суб'єкт даних не має права отримувати від контролера більше інформації, ніж передбачено положеннями національного законодавства держави-члена, що регулюють обмін інформацією між сторонами судових спорів.

14. Хоча мета надання права на доступ є широкою, Суд ЄС проілюстрував також межі сфери дії законодавства про захист даних та права на доступ. Наприклад, Суд ЄС встановив, що мету права на доступ, гарантованого законодавством ЄС про захист даних, слід відрізняти від мети права на доступ до публічних документів, встановленого законодавством ЄС та національним законодавством, оскільки останнє має на меті «максимально можливу прозорість процесу прийняття рішень органами державної влади та сприяння належній адміністративній практиці»[11], що не є метою законодавства про захист даних. Суд ЄС дійшов висновку, що право на доступ до персональних даних застосовується незалежно від того, чи застосовується інший вид права на доступ з іншою метою, наприклад, у контексті процедури експертизи.

[9] Питання, пов'язані із цією темою, є предметом розгляду у справі, яка наразі перебуває на розгляді в Суду ЄС (C-307/22).

[10] Настанови EDPB 10/2020 щодо обмежень, передбачених статтею 23 GDPR, версія для публічних консультацій, 18 грудня 2020 року.

[11] Суд ЄС, об'єднані справи C-141/12 та C-372/12, YS та інші, п. 47.

2.2 Структура статті 15 GDPR

15. Для того, щоб відповісти на запит про отримання доступу й переконатися, що жоден із його аспектів не буде проігнорований, необхідно спочатку зрозуміти структуру статті 15 та складові компоненти права на доступ, передбачені цією статтею.

16. Статтю 15 можна розбити на вісім різних аспектів, перерахованих у таблиці нижче:

1.	Підтвердження того, чи обробляє контролер персональні дані, що стосуються особи, яка подала запит	стаття 15(1), перша половина речення
2.	Доступ до персональних даних, що стосуються особи, яка подала запит	стаття 15(1), перша половина речення (перша частина)
3.	Доступ до такої інформації про обробку: (a) цілі обробки; (b) категорії персональних даних; (c) одержувачі або категорії одержувачів; (d) передбачувана тривалість обробки або критерії для визначення тривалості; (e) наявність прав на виправлення, видалення, обмеження обробки та заперечення проти обробки; (f) право подати скаргу до наглядового органу; (g) будь-яка доступна інформація про джерело даних, якщо вони не були отримані від суб'єкта даних; (h) наявність автоматизованого прийняття рішень, включаючи профайлінг та іншу пов'язану з ним інформацію.	стаття 15(1), друга половина речення (друга частина)
4.	Інформація про гарантії відповідно до статті 46, якщо персональні дані передаються до третьої країни або міжнародної організації	стаття 15(2)
5.	Обов'язок контролера надавати копію персональних даних, що підлягають обробці	стаття 15(3), перше речення
6.	Стягнення контролером обґрунтованої плати на основі адміністративних витрат за будь-які додаткові копії, запитувані суб'єктом персональних даних	стаття 15(3), друге речення
7.	Надання інформації в електронному вигляді	стаття 15(3), третє речення
8.	Врахування прав і свобод інших осіб	стаття 15(4)

Хоча всі аспекти статті 15(1) і (2) разом визначають зміст права на доступ, стаття 15(3) стосується форм доступу, на додаток до загальних вимог, викладених у статті 12 GDPR. Стаття 15(4) доповнює ліміти та обмеження, передбачені статтею 12(5) GDPR для всіх прав суб'єктів даних, з особливим акцентом на права та свободи інших осіб у контексті доступу.

2.2.1 Визначення змісту права на доступ до інформації

17. Стаття 15(1) і (2) містить такі три аспекти: по-перше, підтвердження того, чи обробляються персональні дані запитувача, якщо так, по-друге, доступ до цих даних, і, по-третє, інформація про обробку. Їх можна розглядати як три різні компоненти, які разом складають право на доступ.

2.2.1.1 Підтвердження того, «чи» обробляються персональні дані

18. Подаючи запит на отримання доступу до персональних даних, перше, що потрібно знати суб'єктам даних, — це те, чи обробляє контролер дані, які їх стосуються. Отже, ця інформація є першим компонентом права на доступ відповідно до статті 15(1). Якщо контролер не обробляє персональні дані, що стосуються суб'єкта даних, який запитує доступ, інформація, яку необхідно надати, буде обмежена підтвердженням того, що персональні дані, які стосуються суб'єкта даних, не обробляються. Якщо контролер обробляє дані, що стосуються особи, яка подала запит, контролер повинен підтвердити цей факт цій особі. Таке підтвердження може бути повідомлене окремо або включене в інформацію про персональні дані, що обробляються (див. нижче).

2.2.1.2 Доступ до персональних даних, що обробляються

19. Доступ до персональних даних є другим компонентом права на доступ відповідно до статті 15(1) і становить основу цього права. Це стосується поняття персональних даних, визначеного статтею 4(1) GDPR. Окрім основних персональних даних, таких як ім'я та адреса, під це визначення може підпадати необмежена кількість даних, за умови, що вони підпадають під матеріальну сферу дії GDPR, зокрема, щодо способу їх обробки (стаття 2 GDPR). Доступ до персональних даних означає доступ до самих персональних даних, а не лише загальний опис даних чи просте посилання на категорії персональних даних, які обробляє контролер. Якщо не застосовуються жодні ліміти чи обмеження[12], суб'єкти даних мають право на доступ до всіх даних, що обробляються стосовно них, або до частини даних, залежно від обсягу запиту (див. розділ 2.3.1). Зобов'язання надати доступ до даних не залежить від типу або джерела цих даних. Воно застосовується в повному обсязі навіть у тих випадках, коли особа, яка подала запит, спочатку надала контролеру дані, оскільки його мета полягає в тому, щоб повідомити суб'єкта даних про фактичну обробку цих даних контролером. Обсяг персональних даних відповідно до статті 15 детально пояснюється в розділах 4.1 та 4.2.

2.2.1.3 Інформація про обробку та права суб'єктів даних

20. Третім компонентом права на доступ є інформація про обробку та права суб'єктів даних, яку контролер повинен надати відповідно до статті 15(a)-(h) та 15(2). Така інформація може ґрунтуватися на тексті, взятому, наприклад, із повідомлення про конфіденційність контролера[13] або із записів контролера про діяльність з обробки, зазначених у статті 30 GDPR, але, можливо, її

---

[12] Див. розділ 6 цих Настанов.

[13] Див. інформацію про це в Настановах щодо прозорості відповідно до Регламенту 2016/679 – схвалених EDPB (далі — «Настанови Робочої групи за статтею 29 щодо прозорості – схвалені EDPB») Робочої групи за статтею 29, РД 260, версія 01, 11 квітня 2018 року.

доведеться оновити та адаптувати до запиту суб'єкта даних. Зміст та ступінь деталізації інформації більш детально описані в розділі 4.3.

2.2.2 Положення про способи надання

21. Стаття 15(3) доповнює вимоги до способів надання відповіді на запит про отримання доступу, викладені в статті 12 GDPR, деякими уточненнями в контексті запитів на отримання доступу.

2.2.2.1 Надання копії

22. Відповідно до першого речення статті 15(3) GDPR, контролер повинен надати безкоштовну копію персональних даних, яких стосується обробка. Таким чином, копія стосується лише другого компонента права на доступ («доступ до оброблених персональних даних», див. вище). Контролер повинен забезпечити, щоб перша копія була безкоштовною, навіть якщо він вважає вартість її відтворення високою (приклад: вартість надання копії запису телефонної розмови).

23. Зобов'язання надати копію слід розуміти не як додаткове право суб'єкта даних, а як спосіб забезпечення доступу до даних. Це посилює право на доступ до даних[14] і допомагає тлумачити це право, оскільки чітко вказує на те, що доступ до даних відповідно до статті 15(1) включає повну інформацію про всі дані й не може розумітися як надання лише резюме даних. Водночас зобов'язання надати копію не має на меті розширити обсяг права на доступ: воно стосується (лише) копії персональних даних, що обробляються, а не обов'язково відтворення оригіналів документів (див. розділ 5, п. 152). У більш загальному сенсі, немає ніякої додаткової інформації, яка повинна надаватися суб'єкту даних при наданні копії: обсяг інформації, яка повинна міститися в копії, є обсягом доступу до даних відповідно до статті 15(1) (другий компонент права на доступ, як зазначено вище, див. п. 19), який включає всю інформацію, необхідну для того, щоб дозволити суб'єкту даних зрозуміти та перевірити законність обробки даних.[15]

24. У світлі вищезазначеного, якщо доступ до даних у розумінні статті 15(1) надається шляхом надання копії, зобов'язання, зазначене у статті 15(3), вважається виконаним. Зобов'язання надати копію слугує цілям права на доступ, щоб дозволити суб'єкту даних бути обізнаним і перевірити законність обробки (преамбула 63). Для досягнення цих цілей суб'єкт даних у більшості випадків повинен бачити інформацію не лише тимчасово. Тому суб'єкт даних повинен мати доступ до інформації шляхом отримання копії персональних даних.

25. З огляду на вищезазначене, поняття копії слід тлумачити в широкому сенсі та включати різні види доступу до персональних даних, якщо вони є повними (тобто включають усі запитувані персональні дані) та є можливими для зберігання суб'єктом персональних даних. Таким чином, вимога про надання копії означає, що інформація про персональні дані, які стосуються особи, яка подає запит, надається суб'єкту даних у спосіб, який дозволяє суб'єкту даних зберегти всю інформацію та повернутися до неї.

---

[14] Зобов'язання надавати копію не згадується в Директиві про захист даних 95/46/ЄС.

[15] Питання, пов'язані з темою цього пункту, є предметом розгляду у справі, яка наразі перебуває на розгляді в Суді ЄС (C-487/21

26. Попри таке широке розуміння копії, а також на те, що вона є основним способом надання доступу, за певних обставин інші способи можуть бути доцільними. Подальші пояснення щодо копій та інших способів надання доступу наведені в розділі 5, зокрема в пунктах 5.2.2-5.2.5.

2.2.2.2 Надання додаткових копій

27. Друге речення статті 15(3) стосується ситуацій, коли суб'єкт даних просить контролера надати більше однієї копії, наприклад, якщо перша копія була загублена або пошкоджена, або якщо суб'єкт даних хоче передати копію іншій особі або наглядовому органу. Виходячи з того, що подальші копії повинні бути надані контролером на вимогу суб'єкта даних, стаття 15(3) визначає, що за будь-яку запитувану додаткову копію контролер може стягувати обґрунтовану плату, що базується на адміністративних витратах (друге речення статті 15(3)).

28. Якщо суб'єкт даних просить надати додаткову копію після того, як було зроблено перший запит, можуть виникнути питання про те, чи слід вважати це новим запитом, або чи хоче суб'єкт даних отримати додаткову копію даних у розумінні другого речення статті 15(3), і в цьому випадку може стягуватися плата за додаткову копію. Відповідь на ці питання залежить виключно від змісту запиту: запит слід тлумачити як запит на отримання додаткової копії, якщо за часом та обсягом він стосується тієї ж обробки персональних даних, що й попередній запит. Однак, якщо суб'єкт даних прагне отримати інформацію про дані, оброблені в інший момент часу або які стосуються іншого набору даних, ніж ті, що запитувалися спочатку, право на отримання безкоштовної копії відповідно до статті 15(3) знову застосовується. Це також діє у випадках, коли суб'єкт даних подав перший запит незадовго до цього. Суб'єкт даних може реалізувати своє право на доступ через наступний запит та отримати безкоштовну копію, якщо тільки запит не вважається надмірним відповідно до статті 12(5), з можливістю стягнення обґрунтованої плати відповідно до статті 12(5)(a) (про надмірність повторних запитів див. розділ 6).

> **Приклад 2:** Клієнт подає запит на отримання доступу до інформації до торгівельної компанії. Через рік після відповіді компанії той самий замовник подає запит на отримання доступу до інформації відповідно до статті 15 до тієї ж компанії. Незалежно від того, чи були нові ділові операції або інші контакти між сторонами після попереднього запиту, цей другий запит слід розглядати як новий запит. Навіть якщо не відбулося жодних змін в обробці даних компанією — що не обов'язково є очевидним для суб'єкта даних — суб'єкт даних має право на отримання безкоштовної копії даних.
>
> **Варіант 1**: Навіть якщо клієнт у вищезазначених випадках подає новий запит, наприклад, лише через тиждень після першого запиту, це цілком може розглядатися як новий запит відповідно до першого речення статті 15(1) і (3), якщо його не слід тлумачити як просте нагадування про перший запит. Що стосується короткого інтервалу та залежно від конкретних обставин нового запиту, його надмірність згідно зі статтею 12(5) є питанням (див. розділ 6).
>
> **Варіант 2**: Запит на «нову копію» інформації, яка вже була надана у вигляді копії у відповідь на попередній запит, наприклад, у випадку, якщо запитувач втратив раніше отриману копію, слід, звичайно, розглядати як запит на додаткову копію, оскільки він стосується попереднього запиту за обсягом і часом обробки.

29. Якщо суб'єкт даних повторно подає перший запит на отримання доступу на підставі того, що отримана відповідь не була повною або що не були наведені причини відмови, цей запит не повинен розглядатися як новий запит, оскільки він є лише нагадуванням про перший незадоволений запит.

30. Що стосується розподілу витрат у разі запиту на отримання додаткової копії, то стаття 15(3) встановлює, що контролер може стягувати обґрунтовану плату, яка базується на адміністративних витратах, спричинених запитом. Це означає, що адміністративні витрати є важливим критерієм для встановлення розміру плати. Водночас плата повинна бути відповідною, беручи до уваги важливість права на доступ як основоположного права суб'єкта даних. Контролер не повинен перекладати накладні витрати або інші загальні витрати на суб'єкта даних, а повинен зосередитися на конкретних витратах, пов'язаних із наданням додаткової копії. При організації цього процесу контролер повинен ефективно використовувати свої людські та матеріальні ресурси, щоб утримувати вартість копії на низькому рівні, в тому числі, якщо контролер залучає зовнішню підтримку.

31. Якщо контролер вирішить стягувати плату, він повинен заздалегідь вказати, що плата буде стягуватися, а також — якомога точніше — суму витрат, яку він планує покласти на суб'єкта даних, щоб дати суб'єкту даних можливість вирішити, чи підтримувати запит, чи відкликати його.

2.2.2.3 Надання інформації у загальноприйнятій електронній формі

32. У разі надходження запиту в електронній формі, інформація повинна бути надана в електронній формі, якщо це можливо і якщо суб'єкт даних не вимагає іншого (див. статтю 12(3) GDPR). Третє речення статті 15(3) доповнює цю вимогу в контексті запитів на отримання доступу, зазначаючи, що контролер додатково зобов'язаний надати відповідь у загальноприйнятій електронній формі, якщо тільки суб'єкт даних не попросить про інше. Стаття 15(3) передбачає, що для контролерів, які можуть отримувати електронні запити, буде можливим надати відповідь на запит у загальноприйнятій електронній формі (детальніше див. розділ 5.2.5). Це положення стосується всієї інформації, яка повинна бути надана відповідно до статті 15(1) і (2). Тому, якщо суб'єкт даних подає запит на отримання доступу до інформації електронними засобами, вся інформація повинна бути надана в загальноприйнятій електронній формі. Питання формату більш детально розглядаються в розділі 5. Контролер повинен, як завжди, вживати належних заходів безпеки, зокрема, коли має справу з особливою категорією персональних даних (див. нижче, п. 2.3.4).

2.2.3 Можливе обмеження права на доступ

33. Зрештою, в контексті права на доступ до інформації, конкретне обмеження передбачено в статті 15(4). У ній зазначено, що необхідно враховувати можливі негативні наслідки для прав і свобод інших осіб. Питання щодо обсягу та наслідків цього обмеження, а також щодо додаткових обмежень, викладених у статті 12(5) GDPR або статті 23 GDPR, пояснюються в розділі 6.

2.3 Загальні принципи права на доступ

34. Коли суб'єкти даних подають запит на отримання доступу до своїх даних, у цілому, інформація, зазначена в статті 15 GDPR, завжди повинна бути надана в повному обсязі. Відповідно, якщо контролер обробляє дані, що стосуються суб'єкта даних, він повинен надати всю інформацію, зазначену в статті 15(1) і, за необхідності, інформацію, зазначену в статті 15(2). Контролер

повинен вжити відповідних заходів для забезпечення того, щоб інформація була повною, правильною та актуальною, максимально наближеною до стану обробки даних на момент отримання запиту[16]. Якщо два або більше контролерів обробляють дані спільно, домовленість спільних контролерів щодо їхніх відповідних обов'язків стосовно реалізації прав суб'єктів даних, особливо щодо відповіді на запити на отримання доступу, не впливає на права суб'єктів даних щодо контролера, до якого вони звертаються зі своїм запитом[17].

2.3.1 Повнота інформації

35. Суб'єкти даних мають право на отримання, за винятками, зазначеними нижче, повного розкриття всіх даних, що їх стосуються (докладніше про обсяг див. розділ 4.2). Якщо суб'єкт даних прямо не вимагає іншого, запит на здійснення права на доступ до інформації слід розуміти в загальному сенсі, що охоплює всі персональні дані, які стосуються суб'єкта даних[18]. Обмеження доступу до частини інформації може розглядатися в таких випадках:

a) Суб'єкт даних чітко обмежив запит до певної підгрупи. Щоб уникнути надання неповної інформації, контролер може розглянути таке обмеження запиту суб'єкта даних, тільки якщо він може бути впевнений, що така інтерпретація відповідає бажанню суб'єкта даних (більш детально див. розділ 3.1.1, п. 51). У цілому, суб'єкт даних не повинен повторювати запит на передачу всіх даних, які він має право отримати.

b) У ситуаціях, коли контролер обробляє велику кількість даних, що стосуються суб'єкта даних, у контролера можуть виникнути сумніви, чи дійсно запит на отримання доступу, виражений у дуже загальних рисах, має на меті отримання інформації про всі види даних, що обробляються, або про всі галузі діяльності контролера в деталях. Це може виникнути, зокрема, в ситуаціях, коли не було можливості надати суб'єкту даних інструменти для конкретизації його запиту із самого початку або коли суб'єкт даних не скористався ними. Тоді контролер стикається з проблемою, як надати повну відповідь, водночас уникаючи створення для суб'єкта даних надлишку інформації, яка його не цікавить і з якою він не може ефективно впоратися. Залежно від обставин і технічних можливостей, цю проблему можна вирішити різними способами, наприклад, шляхом надання інструментів самообслуговування в онлайн-контексті (див. розділ 5 про багаторівневий підхід). Якщо такі рішення не застосовуються, контролер, який обробляє велику кількість інформації, що стосується суб'єкта даних, може попросити суб'єкта даних вказати інформацію або обробку, якої стосується запит, до того, як така інформація буде надана (див. преамбулу 63 GDPR). Прикладом може бути компанія з кількома сферами діяльності або орган державної влади з різними адміністративно-територіальними одиницями, якщо контролер виявив, що в цих філіях обробляється велика кількість даних, що стосуються суб'єкта даних. Крім того, велика кількість даних може оброблятися контролерами, які збирають дані про часті дії суб'єкта даних протягом тривалого періоду часу.

---

[16] Вказівки щодо відповідних заходів див. у розділі 5, п. 123-129

[17] Настанови EDPB 07/2020 щодо понять контролера та оператора в GDPR, п. 162f.. Оператори повинні допомагати контролеру, там же, п. 129.

[18] Детальніше див. розділ 5.2.3 нижче, присвячений темі багаторівневого підходу.

Приклад 3: Орган державної влади обробляє дані про суб'єкта даних у низці різних підрозділів, що стосуються різних контекстів. Управління файлами та їх зберігання частково здійснюється неавтоматизованими засобами, а більшість даних зберігається лише в паперових файлах. Що стосується загального формулювання запиту, то державний орган сумнівається, що суб'єкт даних усвідомлює обсяг запиту, особливо різноманітність операцій з обробки, які він охоплює, обсяг інформації та кількість сторінок, які отримає суб'єкт даних.

Приклад 4: Велика страхова компанія отримує запит на загальний доступ у листі від особи, яка є її клієнтом протягом багатьох років. Попри те, що терміни видалення повністю дотримані, компанія фактично обробляє величезну кількість даних про клієнта, оскільки обробка все ще необхідна для виконання договірних зобов'язань, що випливають із договірних відносин з клієнтом (включаючи, наприклад, триваючі зобов'язання, комунікацію щодо спірних питань з клієнтом і третіми сторонами, ...) або для дотримання юридичних зобов'язань (архівні дані, які повинні зберігатися для цілей оподаткування тощо). У страхової компанії можуть виникнути сумніви щодо того, чи дійсно запит, зроблений у дуже загальних рисах, має на меті охопити всі види цих даних. Це може бути особливо проблематично, якщо страхова компанія має лише поштову адресу суб'єкта даних і тому змушена надсилати будь-яку інформацію на папері. Однак такі ж сумніви можуть виникнути і при наданні інформації іншими способами.

Якщо в таких випадках контролер вирішує попросити суб'єкта даних уточнити запит, щоб виконати свій обов'язок сприяти здійсненню права на доступ (стаття 12(2) GDPR), він повинен одночасно надати змістовну інформацію про свої операції з обробки даних, які можуть стосуватися суб'єкта даних, інформуючи про відповідні напрямки своєї діяльності, бази даних тощо.

Приклад 5: У трудових відносинах, у разі загального формулювання запиту на отримання доступу, *не завжди* зрозуміло, що працівник хоче отримати всі дані для входу в систему, дані про доступ до робочого місця, дані про розрахунки в їдальні, дані про виплату заробітної плати тощо. Запит роботодавця на деталізацію може, зокрема, призвести до з'ясування того, що інтерес працівника полягає в тому, щоб зрозуміти або перевірити, кому була передана оцінка його роботи. Без запиту на уточнення працівник отримав би велику кількість інформації, не будучи зацікавленим у більшості даних. Водночас роботодавець повинен надати інформацію про різні контексти обробки, які можуть стосуватися працівника, щоб працівник міг обґрунтовано сформулювати свій запит.

Важливо підкреслити, що запит на уточнення не повинен мати на меті обмеження відповіді на запит про отримання доступу й не повинен використовуватися для приховування будь-якої інформації про дані або обробку, що стосується суб'єкта даних. Якщо суб'єкт даних, якому було запропоновано уточнити обсяг запиту, підтверджує бажання отримати всі персональні дані, що стосуються його або її, контролер, звичайно, повинен надати їх у повному обсязі.

У будь-якому випадку, контролер завжди повинен бути в змозі довести, що спосіб обробки запиту спрямований на максимально широке застосування права на доступ і що він відповідає його зобов'язанням сприяти реалізації прав суб'єктів даних (стаття 12(2) GDPR). З урахуванням

цих принципів, контролер може очікувати відповіді суб'єкта даних, перш ніж надавати додаткові дані відповідно до бажання суб'єкта даних, якщо контролер надав суб'єкту даних чіткий огляд усіх операцій з обробки, які можуть стосуватися суб'єкта даних, включаючи особливо ті, яких суб'єкт даних міг не очікувати, якщо контролер також надав доступ до всіх даних, які суб'єкт даних чітко прагнув отримати, і якщо, крім того, ця інформація була поєднана із чіткими вказівками щодо того, як отримати доступ до решти частин оброблених даних.

c) До права на доступ застосовуються винятки або обмеження (див. нижче в розділі 6). У таких випадках контролер повинен ретельно перевірити, яких частин інформації стосується виняток, і надати всю інформацію, яка не виключається винятком. Наприклад, підтвердження самої обробки персональних даних (компонент 1) може не підпадати під дію винятку. Як наслідок, необхідно надати інформацію про всі персональні дані та всю інформацію, зазначену в статті 15(1) та (2), яких не стосується виняток або обмеження.

2.3.2 Правильність інформації

36. Інформація, що міститься в копії персональних даних, яка надається суб'єкту даних, повинна містити актуальну інформацію або персональні дані, що зберігаються про суб'єкта даних. Це включає обов'язок надавати інформацію про неточні дані або обробку даних, яка не є законною або більше не є законною. Суб'єкт даних може, наприклад, скористатися правом на доступ, щоб дізнатися про джерело неточних даних, які циркулюють між різними контролерами. Якщо контролер виправив неточні дані до того, як поінформував про це суб'єкта даних, суб'єкт даних буде позбавлений цієї можливості. Те саме стосується незаконної обробки. Можливість знати про незаконну обробку, що стосується суб'єкта даних, є однією з основних цілей права на доступ. Обов'язок інформувати про незмінний стан обробки не впливає на обов'язок контролера припинити незаконну обробку або виправити неточні дані. Відповіді на питання про порядок виконання цих зобов'язань наведені нижче.

2.3.3 Часовий орієнтир оцінки

37. Оцінка даних, що обробляються, повинна якомога точніше відображати ситуацію, коли контролер отримує запит, а відповідь повинна охоплювати всі дані, доступні на той момент часу. Це означає, що контролер повинен намагатися дізнатися про всю діяльність з обробки даних, що стосується суб'єкта даних, без невиправданої затримки. Таким чином, контролери не зобов'язані надавати персональні дані, які вони обробляли в минулому, але яких вони більше не мають у своєму розпорядженні[19]. Наприклад, контролер міг видалити персональні дані відповідно до своєї політики зберігання даних та/або законодавчих положень і, таким чином, більше не може надати запитувані персональні дані. У цьому контексті слід нагадати, що тривалість зберігання даних повинна бути зафіксована відповідно до статті 5(1)(e) GDPR, оскільки будь-яке зберігання даних має бути об'єктивно виправданим.

---

[19] Див. із цього приводу подальші роз'яснення в розділі 4 цих настанов, а також рішення Суду Європейського Союзу, C-553/07, 7 травня 2009 року, *College van burgemeester en wethouders van Rotterdam проти M. E. E. Rijkeboer* про право на доступ до інформації щодо одержувачів або категорії одержувачів щодо минулого.

38. Водночас контролер повинен заздалегідь вжити необхідних заходів, щоб полегшити реалізацію права на доступ і розглядати такі запити в найкоротші терміни (див. статтю 12(3)) і до того, як дані будуть видалені. Таким чином, у випадку коротких термінів зберігання, заходи, що вживаються для відповіді на запит, повинні бути адаптовані до відповідного періоду зберігання, щоб полегшити реалізацію права на доступ та уникнути постійної неможливості надання доступу до даних, що обробляються на момент запиту[20]. Однак у деяких випадках може бути неможливо відповісти на запит до настання запланованого терміну видалення даних. Наприклад, якщо під час надання відповіді на запит якнайшвидше, контролер отримує персональні дані, які планувалося видалити наступного дня, йому може знадобитися додатковий час, щоб обміркувати, чи потрібно вносити зміни для захисту свобод інших осіб, перш ніж надати копію персональних даних запитувачу. Якщо дані були отримані протягом запланованого періоду зберігання, контролер може продовжити обробку цих даних з метою виконання свого зобов'язання відповісти на запит. Обробка в таких випадках може ґрунтуватися на статті 6(1)(c) у поєднанні зі статтею 15 GDPR, а її тривалість повинна відповідати вимогам статті 12(3) GDPR[21]. Застосування цієї законної підстави обмежується обробкою даних, визначених як необхідні для відповіді на конкретний запит, і не повинно використовуватися як обґрунтування загальних термінів зберігання даних.

39. Крім того, контролер не повинен навмисно ухилятися від обов'язку надати запитувані персональні дані шляхом видалення або зміни персональних даних у відповідь на запит про отримання доступу (див. 2.3.2). Якщо в процесі обробки запиту на отримання доступу контролер виявить неточні дані або незаконну обробку, він повинен оцінити стан обробки та повідомити про це суб'єкта даних, перш ніж виконувати інші свої зобов'язання. У власних інтересах, щоб уникнути необхідності подальшого спілкування із цього приводу, а також для дотримання принципу прозорості, контролер повинен додати інформацію про подальші виправлення або видалення.

> **Приклад 6**: Відповідаючи на запит про отримання доступу, контролер виявляє, що заявка суб'єкта даних на вакансію в компанії контролера зберігається понад встановлений термін зберігання. У цьому випадку контролер не може спочатку видалити, а потім відповісти суб'єкту даних, що дані (що стосуються заяви) не обробляються. Він повинен спочатку надати доступ, а потім видалити дані. Для того, щоб запобігти подальшому запиту на видалення, рекомендується додати інформацію про факт і час видалення.

З метою дотримання принципу прозорості, контролери повинні інформувати суб'єкта даних про конкретний момент обробки, до якого відноситься відповідь контролера. У деяких випадках, наприклад, у контексті частої комунікаційної діяльності, між цією точкою відліку часу, в якій була

[20] Наприклад, можна розглянути можливість впровадження інструменту самообслуговування, який дозволить суб'єкту даних легко отримати доступ до запитуваних персональних даних, а також системи сповіщення контролера про запит, який стосується персональних даних з коротким терміном зберігання, з метою сприяння оперативному реагуванню.

[21] Це не перешкоджає подальшій обробці даних для цілей доказування у зв'язку з обробкою запиту на отримання доступу протягом відповідного періоду часу.

проведена оцінка обробки, та відповіддю контролера може відбутися додаткова обробка або зміна даних. Якщо контролеру відомо про такі зміни, рекомендується включити інформацію про ці зміни, а також інформацію про додаткову обробку, необхідну для відповіді на запит.

2.3.4 Дотримання вимог безпеки даних

40. Оскільки повідомлення та надання доступу до персональних даних суб'єкту даних є операцією з обробки, контролер завжди зобов'язаний вживати відповідних технічних та організаційних заходів для забезпечення рівня безпеки, що відповідає ризику обробки (див. статтю 5(1)(f), 24 і 32 GDPR). Це застосовується незалежно від способу надання доступу. У разі неелектронної передачі даних суб'єкту даних, залежно від ризиків, пов'язаних з обробкою, контролер може розглянути можливість використання рекомендованої пошти або, як альтернативи, запропонувати, але не зобов'язати суб'єкта даних забрати файл під підпис безпосередньо в одній з установ контролера. Якщо, відповідно до статті 12(1) і (3), інформація надається електронними засобами, контролер повинен вибрати електронні засоби, які відповідають вимогам безпеки даних. Також у разі надання копії даних у загальноприйнятій електронній формі (див. статтю 15(3)), контролер повинен враховувати вимоги безпеки даних при виборі способу передачі електронного файлу суб'єкту даних. Це може включати застосування шифрування, захист паролем тощо. Щоб полегшити доступ до зашифрованих даних, контролер також повинен забезпечити надання відповідної інформації, щоб суб'єкт даних міг отримати доступ до розшифрованої інформації. У випадках, коли вимоги безпеки даних вимагають наскрізного шифрування електронної пошти, але контролер може надіслати лише звичайний електронний лист, контролер повинен використовувати інші засоби, наприклад, надіслати суб'єкту даних USB-накопичувач (рекомендованим листом).

3 ЗАГАЛЬНІ ПОЛОЖЕННЯ ЩОДО ОЦІНКИ ЗАПИТІВ НА ОТРИМАННЯ ДОСТУПУ

3.1 Вступ

41. При надходженні запитів на отримання доступу до персональних даних контролер повинен оцінювати кожен запит окремо. Контролер повинен взяти до уваги, *серед іншого,* такі питання, які розглядаються в наступних пунктах: чи стосується запит персональних даних, пов'язаних із особою, яка подає запит, і хто така особа, яка подає запит. Цей розділ має на меті роз'яснити, які аспекти запиту на отримання доступу повинен враховувати контролер під час його оцінки, та обговорити можливі сценарії такої оцінки, а також її наслідки. Контролер, оцінюючи запит на отримання доступу до персональних даних, повинен також враховувати, відповідно до статті 12(2) GDPR, обов'язок сприяти реалізації прав суб'єкта персональних даних, не забуваючи при цьому про належну безпеку персональних даних[22].

[22] Контролер повинен забезпечити належну безпеку персональних даних відповідно до принципу цілісності та конфіденційності (стаття 5(1)(f) GDPR), впроваджуючи відповідні технічні та організаційні

42. Тому контролери повинні бути готовими до обробки запитів на отримання доступу до персональних даних. Це означає, що контролер повинен бути готовий отримати запит, належним чином оцінити його (ця оцінка є предметом цього розділу настанов) та надати відповідну відповідь без невиправданої затримки особі, яка подала запит. Спосіб підготовки контролерів до виконання запитів на отримання доступу повинен бути адекватним та обґрунтованим і залежати від специфіки, обсягу, контексту та цілей обробки, а також ризиків для прав і свобод фізичних осіб, відповідно до статті 24 GDPR. Залежно від конкретних обставин, контролери можуть, наприклад, бути зобов'язані впровадити відповідну процедуру, реалізація якої повинна гарантувати безпеку даних, не перешкоджаючи здійсненню прав суб'єкта даних.

3.1.1 Аналіз змісту запиту

43. Це питання можна більш конкретно оцінити, поставивши такі запитання.

a) Чи стосується запит персональних даних?

44. Відповідно до GDPR, сфера дії запиту повинна охоплювати лише персональні дані[23]. Тому будь-який запит на отримання інформації з інших питань, включаючи загальну інформацію про контролера, його бізнес-моделі або діяльність з обробки, не пов'язану з персональними даними, не слід розглядати як запит, поданий відповідно до статті 15 GDPR. Крім того, запит на інформацію про знеособлені дані або дані, які не стосуються особи, яка подає запит, або особи, від імені якої уповноважена особа подала запит, не підпадає під сферу дії права на доступ. Це питання буде більш детально проаналізовано в розділі 4.

45. На відміну від знеособлених даних (які не є персональними даними), псевдонімізовані дані, які можуть бути пов'язані з фізичною особою за допомогою додаткової інформації, є персональними даними[24]. Таким чином, псевдонімізовані дані, які можуть бути пов'язані із суб'єктом даних — наприклад, коли суб'єкт даних надає відповідний ідентифікатор, що дозволяє його ідентифікувати, або коли контролер може пов'язати дані з особою, яка подала запит, власними засобами — повинні розглядатися в рамках запиту[25].

b) Чи стосується запит особи, яка подає запит (або особи, від імені якої уповноважена особа подає запит)?

заходи, як зазначено в статті 32 GDPR та деталізовано у статті 24 GDPR. Контролер повинен довести, що він забезпечує належний рівень захисту даних відповідно до принципу підзвітності (див. також: Висновок 3/2010 Робочої групи за статтею 29 щодо принципу підзвітності, прийнятого 13 липня 2010 року, 00062/10/EN РД 173 та Настанови EDPB № 07/2020 щодо понять контролера та оператора в GDPR).

[23] За винятком випадків, коли запит стосується також неперсональних даних, нерозривно пов'язаних із персональними даними суб'єкта даних. Додаткові пояснення див. у пункті 100.

[24] Див. преамбулу 26 GDPR. Додаткові пояснення щодо понять знеособлених даних та псевдонімізованих даних можна знайти у Висновку 4/2007 Робочої групи за статтею 29 щодо поняття персональних даних, с. 18-21.

[25] Настанови щодо права на перенесення даних Робочої групи за статтею 29, РД 24, версія 01, 5 квітня 2017 року – схвалені EDPB (далі — «Настанови робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB»), с. 9.

46. Як правило, запит може стосуватися лише даних особи, яка подає запит. Доступ до даних інших осіб можна запитувати лише за наявності відповідного дозволу[26].

> **Приклад 7:** Суб'єкт даних X працює менеджером відділу в компанії, яка надає паркувальні місця для своїх менеджерів на автостоянці компанії. Хоча у суб'єкта даних X є постійне місце для паркування, коли він приїжджає в офіс на другу зміну, це місце часто вже зайняте іншим автомобілем. Оскільки ця ситуація повторюється, для того, щоб ідентифікувати водія, який без дозволу займає його місце, суб'єкт даних просить контролера системи відеоспостереження, що охоплює територію парковки офісу, надати доступ до персональних даних цього водія. У такому випадку запит суб'єкта даних X не буде запитом на отримання доступу до його персональних даних, оскільки запит стосується не даних запитувача, а даних іншої особи — і тому його не слід вважати запитом відповідно до статті 15 GDPR.

c) Чи застосовуються інші положення, крім GDPR, що регулюють доступ до певної категорії даних?

47. Суб'єкти даних не зобов'язані вказувати законну підставу у своєму запиті. Однак, якщо суб'єкти даних уточнюють, що їхній запит ґрунтується на галузевому законодавстві або національному законодавстві, що регулює конкретне питання доступу до певних категорій даних, а не на GDPR, такий запит повинен бути розглянутий контролером відповідно до таких галузевих або національних правил, за необхідності. Часто, залежно від відповідного національного законодавства, від контролерів може вимагатися надання окремих відповідей, кожна з яких стосується конкретних вимог, викладених у різних законодавчих актах. Їх не слід плутати з національним законодавством або законодавством ЄС, що встановлює обмеження на право на доступ, яких необхідно дотримуватися при наданні відповідей на запити на отримання доступу.

48. Якщо контролер має сумніви щодо того, яким правом хоче скористатися суб'єкт даних, рекомендується звернутися до суб'єкта даних, який подає запит, з проханням пояснити предмет запиту. Таке листування із суб'єктом даних не впливає на обов'язок контролера діяти без невиправданої затримки[27]. Однак у разі виникнення сумнівів, якщо контролер звертається до суб'єкта даних за додатковими поясненнями та не отримує відповіді, пам'ятаючи про обов'язок сприяти здійсненню особою права на доступ, контролер повинен інтерпретувати інформацію, що міститься в першому запиті, і діяти на цій основі. Відповідно до принципу підзвітності, контролер може визначити відповідний термін, протягом якого суб'єкт даних може надати додаткові пояснення. Встановлюючи такі часові рамки, контролер повинен залишити достатньо часу для виконання запиту після його закінчення, а отже, враховувати, скільки часу об'єктивно необхідно для збору та надання запитуваних даних після того, як суб'єкт даних надав (або не надав) специфікацію.

49. Якщо запит підпадає під сферу дії GDPR, існування такого окремого законодавства не скасовує загального застосування права на доступ, передбаченого GDPR. Можуть існувати обмеження,

---

[26] Див. розділ 3.4 («Запити, зроблені через третіх осіб/довірених осіб»).

[27] Див. подальші вказівки щодо термінів у розділі 5.3.

встановлені законодавством ЄС або національним законодавством, якщо це дозволено статтею 23 GDPR (див. розділ 6.4).

d) Чи підпадає запит під дію статті 15?

50. Слід зазначити, що GDPR не встановлює жодних формальних вимог до осіб, які подають запит на отримання доступу до даних. Для того, щоб подати запит на отримання доступу до даних, запитувачу достатньо вказати, що він хоче знати, які персональні дані, що стосуються його, обробляє контролер. Тому контролер не може відмовити в наданні даних, посилаючись на відсутність вказівки на законну підставу запиту, особливо на відсутність конкретного посилання на право на доступ або GDPR.

Наприклад, для того, щоб подати запит, особі, яка його подає, достатньо вказати, що:

- особа бажає отримати доступ до персональних даних, які її стосуються;
- особа реалізує своє право на доступ; або
- особа бажає знати інформацію про себе, яку обробляє контролер.

Слід мати на увазі, що заявники можуть бути не знайомі з тонкощами GDPR і що бажано бути поблажливими до осіб, які реалізують своє право на доступ, зокрема, коли воно реалізується неповнолітніми. Як зазначено вище, у разі будь-яких сумнівів контролеру рекомендується попросити суб'єкта даних, який подає запит, уточнити предмет запиту.

e) Чи хочуть суб'єкти даних отримати доступ до всієї або частини інформації, що обробляється про них?

51. Крім того, контролер повинен оцінити, чи стосуються запити, зроблені запитувачами, всієї або частини інформації, що обробляється про них. Будь-яке обмеження обсягу запиту конкретним положенням статті 15 GDPR, зроблене суб'єктами даних, має бути чітким і недвозначним. Наприклад, якщо суб'єкти даних вимагають дослівно «інформацію про дані, що обробляються стосовно них», контролер повинен виходити з того, що суб'єкти даних мають намір скористатися своїм повним правом, передбаченим статтею 15(1)-(2) GDPR. Такий запит не слід тлумачити як такий, що суб'єкти даних бажають отримувати лише ті категорії персональних даних, які обробляються, і відмовляються від свого права на отримання інформації, перерахованої в статті 15(1)(a)-(h). Ситуація може бути іншою, наприклад, якщо суб'єкти даних бажають мати доступ до джерела або походження персональних даних або до зазначеного періоду їх зберігання, стосовно даних, які вони вказують. У такому випадку контролер може обмежити свою відповідь конкретною запитуваною інформацією.

3.1.2 Форма запиту

52. Як зазначалося раніше, GDPR не висуває жодних вимог до суб'єктів даних щодо форми запиту на отримання доступу до персональних даних. Тому, загалом, не існує вимог GDPR, яких суб'єкти даних повинні дотримуватися при виборі каналу зв'язку, за допомогою якого вони вступають у контакт з контролером.

53. EDPB закликає контролерів надавати найбільш підходящі та зручні для користувача канали зв'язку відповідно до статті 12(2) та статті 25 GDPR, щоб дозволити суб'єкту даних надати результативний запит. Проте, якщо суб'єкт даних подає запит, використовуючи канал зв'язку,

наданий контролером[28], який відрізняється від того, що вказаний як бажаний, такий запит, як правило, вважається результативним, і контролер повинен обробити такий запит відповідним чином (див. приклади нижче). Контролери повинні докладати всіх необхідних зусиль для того, щоб полегшити здійснення прав суб'єктів даних (наприклад, коли суб'єкт даних надсилає запит на отримання доступу до даних працівнику, який перебуває у відпустці, обґрунтованим кроком може бути автоматичне повідомлення, що інформує суб'єкта даних про альтернативний канал зв'язку для цього запиту).

54. Слід зазначити, що контролер не зобов'язаний реагувати на запит, надісланий на випадкову або неправильну електронну (або поштову) адресу, не надану безпосередньо контролером, або на будь-який канал зв'язку, який явно не призначений для отримання запитів, що стосуються прав суб'єкта даних, якщо контролер надав відповідний канал зв'язку, який може бути використаний суб'єктом даних.

55. Контролер також не зобов'язаний діяти на запит, надісланий на електронну адресу працівника контролера, який не може бути залучений до обробки запитів, що стосуються прав суб'єктів даних (наприклад, водії, прибиральники тощо). Такі запити не вважаються результативними, якщо контролер чітко надав суб'єкту даних відповідний канал зв'язку. Однак, якщо суб'єкт даних надсилає запит працівнику контролера, який був призначений як постійна контактна особа (наприклад, менеджер персонального рахунку в банку або постійний консультант оператора мобільного зв'язку), такий контакт не повинен розглядатися як випадковий, і контролер повинен докласти всіх необхідних зусиль, щоб обробити цей запит таким чином, щоб його можна було перенаправити до контактної особи та відповісти на нього у строки, передбачені GDPR.

56. Однак EDPB рекомендує, як належну практику, щоб контролери запровадили відповідні механізми для полегшення реалізації прав суб'єктів даних, включаючи системи автовідповідачів для інформування про відсутність персоналу та відповідні альтернативні контакти, а також, за можливості, механізми для покращення внутрішньої комунікації між працівниками щодо запитів, отриманих тими, хто може бути некомпетентним для розгляду таких запитів.

> **Приклад 8**: Контролер С вказує на своєму вебсайті та у повідомленні про конфіденційність дві адреси електронної пошти: загальну адресу електронної пошти контролера: CONTACT@C.COM та адресу електронної пошти контактної особи контролера з питань захисту даних: QUERIES@C.COM. Крім того, контролер С вказує на своєму вебсайті, що для подання будь-яких запитів або запитів щодо обробки персональних даних фізичні особи повинні звертатися до контактної особи з питань захисту даних за вказаною адресою електронної пошти. Однак суб'єкт даних надсилає запит на загальну електронну адресу контролера: CONTACT@C.COM.

[28] Це можуть бути, зокрема, комунікаційні дані контролера, надані в його повідомленнях, адресованих безпосередньо суб'єктам даних, або контактні дані, надані контролером публічно, наприклад, у політиці конфіденційності контролера або інших обов'язкових юридичних повідомленнях контролера (зокрема контактна інформація про власника або компанію на вебсайті).

У такому випадку контролер повинен докласти всіх необхідних зусиль, щоб його служби знали про запит, який був зроблений через загальну електронну пошту, щоб його можна було перенаправити до контактного пункту захисту даних і відповісти на нього у терміни, передбачені GDPR. Крім того, контролер не має права продовжувати термін відповіді на запит лише тому, що суб'єкт даних надіслав запит на загальну електронну адресу контролера, а не на електронну адресу контактного пункту контролера із захисту даних.

Приклад 9: Контролер Y керує мережею фітнес-клубів. Контролер Y вказує на своєму вебсайті та в повідомленні про конфіденційність для клієнтів фітнес-клубу, що для подання будь-яких запитів або запитів щодо обробки персональних даних фізичні особи повинні звертатися до контролера за електронною адресою QUERIES@Y.COM. Одна суб'єкт даних надсилає запит на електронну адресу, знайдену в роздягальні, де він виявив повідомлення такого змісту: «Якщо ви не задоволені чистотою приміщення, будь ласка, зв'яжіться з нами за адресою: CLEANERS@Y.COM», що є електронною адресою прибиральниць, яких наймає контролер Y. Очевидно, що прибиральниці не залучені до вирішення питань, пов'язаних із реалізацією прав суб'єктів даних — клієнтів фітнес-клубу. Хоча адреса електронної пошти була доступна на території фітнес-клубу, суб'єкт даних не міг обґрунтовано очікувати, що це належна контактна адреса для таких запитів, оскільки вебсайт і повідомлення про конфіденційність чітко інформували про канал зв'язку, який буде використовуватися для реалізації прав суб'єктів даних.

57. Дата отримання запиту контролером, як правило, є початком відліку місячного строку, протягом якого контролер повинен надати інформацію про дії, вжиті за запитом, відповідно до статті 12(3) GDPR (подальші вказівки щодо термінів надаються в розділі 5.3). EDPB вважає належною практикою для контролерів підтверджувати отримання запитів у письмовій формі, наприклад, надсилаючи електронні листи (або інформацію поштою, якщо це можливо) запитувачам, підтверджуючи, що їхні запити були отримані та що місячний період триває з дня X по день Y.

3.2 Ідентифікація та автентифікація

58. З метою забезпечення безпеки обробки та мінімізації ризику несанкціонованого розкриття персональних даних контролер повинен мати можливість з'ясувати, які дані стосуються суб'єкта даних (ідентифікація) та підтвердити цю особу (автентифікація).

59. Слід нагадати, що в ситуаціях, коли мета, для якої обробляються персональні дані, не вимагає або більше не вимагає ідентифікації суб'єкта даних, контролер не зобов'язаний зберігати ідентифікацію виключно з метою дотримання прав суб'єктів даних, а також у світлі принципу мінімізації даних. Ці ситуації розглядаються в статті 11(1) GDPR.

60. У статті 12(2) GDPR зазначає, що контролер не повинен відмовлятися діяти на запит суб'єкта даних для реалізації його прав, за винятком випадків, коли контролер обробляє персональні дані з метою, яка не вимагає ідентифікації суб'єкта даних, і він доводить, що не має можливості

ідентифікувати суб'єкта даних. За таких обставин суб'єкт даних може, однак, прийняти рішення про надання додаткової інформації, яка дозволить його ідентифікувати (стаття 11(2) GDPR)[29].

61. Контролер не зобов'язаний отримувати таку додаткову інформацію для ідентифікації суб'єкта даних виключно з метою виконання запиту суб'єкта даних, також у світлі принципу мінімізації даних. Однак він не повинен відмовлятися від отримання такої додаткової інформації, наданої суб'єктом даних для підтримки реалізації його прав (стаття 57 GDPR).

Приклад 10: Контролер С є контролером даних, що обробляються у зв'язку з відеоспостереженням будівлі. Відповідно до статті 11(1) GDPR, контролер не зобов'язаний ідентифікувати всіх осіб, які були зареєстровані камерою спостереження в рамках моніторингу (мета, що не вимагає ідентифікації). Контролер отримує запит на отримання доступу до персональних даних від особи, яка стверджує, що була зафіксована камерою відеоспостереження контролера. Дії контролера залежать від наданої додаткової інформації. Якщо запитувач вкаже конкретний день і час, коли камери могли зафіксувати подію, про яку йдеться, ймовірно, що контролер зможе надати такі дані (стаття 11(2) GDPR). Однак, якщо контролер не може ідентифікувати суб'єкта даних (наприклад, якщо контролер не може бути впевнений, що особа, яка подала запит, дійсно є суб'єктом даних, або якщо запит стосується, наприклад, тривалого періоду записів і контролер не в змозі обробити таку велику кількість даних), контролер може відмовити у виконанні запиту, якщо доведе, що він не в змозі ідентифікувати суб'єкта даних (стаття 12(2) GDPR).

Приклад 11: Контролер С обробляє персональні дані з метою показу поведінкової реклами своїм вебкористувачам. Персональні дані, зібрані для поведінкової реклами, зазвичай збираються за допомогою файлів cookie і пов'язуються із псевдонімами та випадковими ідентифікаторами. Суб'єкт даних пан Х реалізує своє право на доступ до контролера С через вебсайт контролера С. Контролер С може точно ідентифікувати пана Х для показу поведінкової реклами суб'єкта даних, пов'язуючи термінальне обладнання пана Х з його рекламним профілем за допомогою файлів cookie, скинутих на термінал. Контролер С також повинен точно ідентифікувати пана Х, щоб надати йому доступ до його персональних даних, оскільки можна знайти зв'язок між обробленими даними та суб'єктом даних. Тому, беручи до уваги принципи GDPR, наведений вище приклад не підпадає під дію статті 11 GDPR. Точніше кажучи, у наведеному вище прикладі цілі контролера С вимагають ідентифікації суб'єктів даних, тоді як стаття 11 GDPR розглядає ситуацію з обробки, яка не вимагає ідентифікації, коли контролер не зобов'язаний обробляти додаткові дані в розумінні статті 11(1) GDPR з єдиною метою дотримання вимог GDPR. Отже, в деяких випадках для реалізації прав суб'єкта даних не потрібно запитувати додаткові дані.

[29] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 13.

Однак, якщо пан X спробує скористатися своїм правом на доступ електронною поштою або звичайною поштою, то в цьому контексті контролер C не матиме іншого вибору, окрім як попросити пана X надати «додаткову інформацію» (стаття 12(6) GDPR), щоб мати можливість ідентифікувати рекламний профіль, пов'язаний із паном X. У цьому випадку додатковою інформацією буде ідентифікатор файлу cookie, який зберігається в термінальному обладнанні пана X.

62. У разі доведеної неможливості ідентифікувати суб'єкта даних (стаття 11 GDPR), контролер повинен поінформувати про це суб'єкта даних, якщо це можливо, оскільки контролер повинен відповідати на запити суб'єкта даних без невиправданої затримки та надавати причини, якщо він не має наміру виконувати такі запити. Цю інформацію потрібно надавати лише «якщо це можливо», оскільки контролер може бути не в змозі інформувати суб'єктів даних, якщо їхня ідентифікація неможлива.

63. Як у випадках, коли обробка не вимагає ідентифікації, так і в тих випадках, коли вона вимагає її, якщо контролер має обґрунтовані сумніви щодо фізичної особи, яка подає запит, він може вимагати надання додаткової інформації, необхідної для підтвердження особи суб'єкта даних (стаття 12(6) GDPR).

64. GDPR не встановлює жодних вимог щодо способу автентифікації суб'єкта даних. Однак, статті 11 і 12 GDPR вказують на умови реалізації всіх прав суб'єкта даних, включаючи право на доступ до персональних даних.

65. Слід пам'ятати, що, як правило, контролер не може запитувати більше персональних даних, ніж це необхідно для забезпечення такої автентифікації, і що використання такої інформації має бути суворо обмежене виконанням запиту суб'єктів даних.

66. Процедури автентифікації часто вже існують між суб'єктами даних та контролерами. Контролери можуть використовувати ці процедури автентифікації для того, щоб встановити особу суб'єктів даних, які запитують свої персональні дані або користуються правами, наданими GDPR[30]. В іншому випадку контролери повинні впровадити процедуру автентифікації для цього[31].

67. У випадках, коли контролер запитує або отримує від суб'єкта даних додаткову інформацію, необхідну для підтвердження особи суб'єкта даних, контролер повинен щоразу оцінювати, яка інформація дозволить йому підтвердити особу суб'єкта даних, і, можливо, поставити додаткові запитання особі, яка подала запит, або попросити суб'єкта даних надати деякі додаткові аспекти ідентифікації, якщо це буде обґрунтованим (див. розділ 3.3).

68. Щоб дозволити суб'єкту даних надати додаткову інформацію, необхідну для ідентифікації його даних, контролер повинен повідомити суб'єкта даних про характер додаткової інформації, необхідної для ідентифікації. Така додаткова інформація не повинна бути більшою, ніж та, яка спочатку необхідна для автентифікації суб'єкта даних. Загалом, той факт, що контролер може вимагати додаткову інформацію для оцінки особи суб'єкта даних, не може призвести до

[30] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 14.

[31] Див. подальші вказівки щодо автентифікації в розділі 3.3.

надмірних вимог та збору персональних даних, які не є релевантними або необхідними для зміцнення зв'язку між особою та запитуваними персональними даними[32].

69. Як наслідок, якщо інформація, зібрана в Інтернеті, пов'язана із псевдонімами або іншими унікальними ідентифікаторами, контролер може запровадити відповідні процедури, які дозволять особі, що подає запит, подати запит на отримання доступу до даних та отримати дані, що її стосуються[33].

> **Приклад 12:** Суб'єкт даних пані Х запитує доступ до своїх даних під час розмови з консультантом гарячої лінії електроенергетичної компанії, з якою вона уклала договір. Консультант, маючи сумніви щодо особи, яка робить запит, генерує в системі компанії одноразовий унікальний код, який надсилається на номер мобільного телефону користувача, наданий при створенні облікового запису, в рамках системи подвійної перевірки, що в цьому випадку слід вважати обґрунтованою дією.

3.3 Оцінка обґрунтованості щодо автентифікації особи, яка подає запит

70. Як зазначено вище, якщо контролер має обґрунтовані підстави сумніватися в особі запитувача, він може запросити додаткову інформацію для підтвердження особи суб'єкта даних. Однак при цьому контролер повинен переконатися, що він не збирає більше персональних даних, ніж це необхідно для автентифікації особи, яка подає запит. Тому контролер повинен провести оцінку обґрунтованості, яка має враховувати тип персональних даних, що обробляються (наприклад, спеціальні категорії даних чи ні), характер запиту, контекст, у якому робиться запит, а також будь-яку шкоду, яка може бути заподіяна в результаті запиту. Оцінюючи обґрунтованість, слід пам'ятати, що необхідно уникати надмірного збору даних, забезпечуючи при цьому належний рівень безпеки обробки.

71. Контролер повинен впровадити процедуру автентифікації для того, щоб бути впевненим в особах, які запитують доступ до своїх даних[34], і забезпечити безпеку обробки протягом усього процесу обробки запитів на отримання доступу відповідно до статті 32 GDPR, включаючи, наприклад, безпечний канал для надання суб'єктами даних додаткової інформації. Метод, що використовується для автентифікації, повинен бути релевантним, відповідним, обґрунтованим та відповідати принципу мінімізації даних. Якщо контролер запроваджує заходи, спрямовані на автентифікацію суб'єкта даних, які є обтяжливими, він повинен належним чином обґрунтувати це та забезпечити дотримання всіх основоположних принципів, включаючи мінімізацію даних та обов'язок сприяти реалізації прав суб'єктів даних (стаття 12(2) GDPR).

---

[32] Там же, с. 14.

[33] Там же, с. 13-14.

[34] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 14.

72. В онлайн-контексті механізм автентифікації може включати ті самі облікові дані, які використовуються суб'єктом даних для входу в онлайн-сервіс, пропонований контролером (стаття 57 GDPR)[35].

73. На практиці процедури автентифікації часто існують, і контролерам не потрібно запроваджувати додаткові гарантії для запобігання несанкціонованому доступу до послуг. Для того, щоб дозволити фізичним особам отримати доступ до даних, що містяться в їхніх облікових записах (таких як обліковий запис електронної пошти, обліковий запис у соціальних мережах або в інтернет-магазинах), контролери, швидше за все, вимагатимуть входу через логін і пароль користувача, які в таких випадках повинні бути достатніми для автентифікації суб'єкта даних[36]. Крім того, суб'єкти даних часто вже автентифіковані контролером до укладення договору або отримання їхньої згоди на обробку, і, як наслідок, персональні дані, що використовуються для реєстрації особи, якої стосується обробка, також можуть бути використані як доказ для автентифікації суб'єкта даних для цілей доступу[37]. Отже, необґрунтовано вимагати копію документа, що посвідчує особу, у випадку, коли суб'єкт даних, який подає запит, вже автентифікований контролером.

74. Слід підкреслити, що використання копії документа, що посвідчує особу, як частини процесу автентифікації створює ризик для безпеки персональних даних і може призвести до несанкціонованої або незаконної обробки, і тому її слід вважати недоцільною, якщо тільки вона не є необхідною, доцільною і не відповідає національному законодавству. У таких випадках контролери повинні мати системи, що забезпечують рівень безпеки, достатній для зменшення підвищених ризиків для прав і свобод суб'єктів даних, які отримують такі дані. Важливо також зазначити, що автентифікація за допомогою посвідчення особи не обов'язково допомагає в онлайн-контексті (наприклад, при використанні псевдонімів), якщо відповідна особа не може надати інші докази, наприклад, додаткові характеристики, що відповідають обліковому запису користувача.

75. Беручи до уваги той факт, що багато організацій (наприклад, готелі, банки, пункти прокату автомобілів) вимагають копії посвідчення особи своїх клієнтів, це, як правило, не слід вважати належним способом автентифікації. Як альтернатива, контролер може запровадити швидкий та ефективний захід безпеки для ідентифікації суб'єкта даних на основі автентифікації, яку він здійснював раніше, наприклад, за допомогою електронної пошти або текстового повідомлення, що містить посилання для підтвердження, питання безпеки або коди підтвердження[38].

---

[35] Додаткові вказівки щодо методів автентифікації див. у Настановах EDPB 01/2021 «Приклади щодо повідомлень про порушення безпеки даних», прийнятих 14 січня 2021 року, с. 30-31, та в Настановах EDPB 02/2021 «Віртуальні голосові помічники», версія 2.0, прийнята 7 липня 2021 року, розділ 3.7.

[36] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 14.

[37] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 14.

[38] Див. також 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 та скасування Директиви 1999/93/ЄС, яка запровадила різні послуги, що дозволяють безпечну віддалену ідентифікацію.

76. Інформація на посвідченні особи, яка не є необхідною для підтвердження особи суб'єкта даних, така як номер доступу та серійний номер, національність, розмір, колір очей, фотографія та машинозчитувана зона, залежно від оцінки кожного конкретного випадку, може бути відредагована або прихована суб'єктом даних перед поданням її контролеру, за винятком випадків, коли національне законодавство вимагає повної невідредагованої копії посвідчення особи (див. пункт 78 нижче). Як правило, дата видачі або закінчення терміну дії, орган, що видав посвідчення, та повне ім'я, що збігається з онлайн-акаунтом, є достатніми для перевірки особи контролером, завжди за умови, що автентичність копії та її зв'язок із заявником забезпечені. Додаткова інформація, така як дата народження суб'єкта даних, може знадобитися лише у випадку, якщо зберігається ризик помилкової ідентифікації, якщо контролер може порівняти її з інформацією, яку він вже обробляє.

77. Щоб дотримуватися принципу мінімізації даних, контролер повинен повідомити суб'єкта даних про інформацію, яка не є необхідною, та про можливість відредагувати або приховати ці частини документа, що посвідчує особу. У такому випадку, якщо суб'єкт даних не знає, як або не може відредагувати таку інформацію, доброю практикою для контролера буде відредагувати її після отримання документа, якщо це можливо для контролера, беручи до уваги засоби, доступні контролеру за даних обставин.

Приклад 13: Користувач пані Y створила захищений паролем обліковий запис в інтернет-магазині, вказавши свою електронну пошту та/або ім'я користувача. Згодом власник облікового запису запитує у контролера інформацію про те, чи обробляє він його персональні дані, і якщо так, то просить надати йому доступ до них в обсязі, зазначеному в статті 15. Контролер запитує посвідчення особи, яка подає запит, щоб підтвердити її особу. Дії контролера в цьому випадку є необґрунтованими та призводять до непотрібного збору даних.

Однак, щоб підтвердити особу, яка подає запит, запобігаючи при цьому непотрібному збору даних, контролер може вимагати від неї автентифікації шляхом входу в обліковий запис або задати їй (ненав'язливі) питання безпеки, відповідь на які повинен знати тільки суб'єкт даних, або використовувати багатофакторну автентифікацію, яка була налаштована при реєстрації облікового запису суб'єкта даних, або використовувати інші існуючі засоби зв'язку, які, як відомо, належать суб'єкту даних, такі як адреса електронної пошти або номер телефону, для надсилання пароля доступу.

Приклад 14: Клієнт банку, пан Y, планує отримати споживчий кредит. Із цією метою пан Y звертається до відділення банку для отримання інформації, в тому числі його персональних даних, необхідної для оцінки його кредитоспроможності. Для перевірки особи суб'єкта даних консультант просить нотаріально засвідчити його особу, щоб мати можливість надати йому необхідну інформацію.

Контролер не повинен вимагати нотаріального підтвердження особи, якщо це не є необхідним, прийнятним і відповідає національному законодавству (наприклад, коли особа тимчасово не має документа, що посвідчує особу, а підтвердження особи суб'єкта даних вимагається національним законодавством для виконання юридичної дії). Така практика наражає запитувачів на додаткові витрати та накладає надмірний тягар на суб'єктів даних, перешкоджаючи здійсненню їхнього права на доступ.

78. Не обмежуючи вищезазначених загальних принципів, за певних обставин автентифікація на основі ідентифікації може бути виправданим та обґрунтованим заходом, зокрема для суб'єктів, які обробляють спеціальні категорії персональних даних або здійснюють обробку даних, які можуть становити ризик для суб'єкта даних (наприклад, медична інформація або інформація про стан здоров'я). Однак водночас слід мати на увазі, що окремі національні положення передбачають обмеження на обробку даних, що містяться в публічних документах, у тому числі в документах, що підтверджують особу (також на підставі статті 87 GDPR). Обмеження на обробку даних із цих документів можуть стосуватися, зокрема, сканування або фотокопіювання посвідчень особи або обробки офіційних персональних ідентифікаційних номерів[39].

79. Беручи до уваги вищезазначене, якщо запитується посвідчення особи (і це відповідає національному законодавству, а також є обґрунтованим і відповідає GDPR), контролер повинен вжити заходів для запобігання незаконній обробці посвідчення особи. Попри будь-які застосовні національні положення щодо автентифікації ідентифікації, це може включати утримання від створення копії або видалення копії ідентифікації одразу після успішної автентифікації особи суб'єкта даних. Це пов'язано з тим, що подальше зберігання копії посвідчення особи може становити порушення принципів обмеження мети та обмеження зберігання (стаття 5(1)(b) та (e) GDPR) і, крім того, національного законодавства щодо обробки національного ідентифікаційного номера (стаття 87 GDPR). EDPB рекомендує, як належну практику, щоб контролер після перевірки документа, що посвідчує особу, робив відмітку, наприклад, «Документ, що посвідчує особу, перевірено», щоб уникнути непотрібного копіювання або зберігання копій таких документів.

3.4 Запити, зроблені через третіх/довірених осіб

80. Хоча право на доступ, як правило, реалізується суб'єктами даних у частині, що їх стосується, третя сторона може подати запит від імені суб'єкта даних. Це може стосуватися, серед іншого, дій через довірену особу або законних опікунів від імені неповнолітніх, а також дій через інших суб'єктів через онлайн-портали. За деяких обставин особа, уповноважена здійснювати право на доступ, а також повноваження діяти від імені суб'єкта даних, може потребувати перевірки, якщо вона є доцільною та обґрунтованою (див. розділ 3.3 вище)[40]. Слід нагадати, що надання доступу

[39] Декілька держав-членів ЄС запровадили таке обмеження у своїх національних положеннях із цього приводу, зазначивши, зокрема, що виготовлення копій посвідчень особи є законним лише тоді, коли це прямо випливає з положень нормативно-правового акта.

[40] Щодо строків реалізації права на доступ, коли контролеру необхідно отримати додаткову інформацію, див. п. 157.

до персональних даних особі, яка не має права на доступ до них, може становити порушення безпеки персональних даних[41].

81. При цьому слід враховувати національне законодавство, що регулює юридичне представництво (наприклад, довіреності), яке може встановлювати конкретні вимоги щодо підтвердження повноважень подавати запит від імені суб'єкта даних, оскільки GDPR не регулює це питання. Відповідно до принципу підзвітності, а також інших принципів захисту даних, контролери повинні довести наявність відповідних повноважень для подання запиту від імені суб'єкта даних та отримання запитуваної інформації, за винятком випадків, коли національне законодавство відрізняється (наприклад, національне законодавство містить спеціальні правила щодо благонадійності адвокатів), що залишає за контролером право перевіряти особу суб'єкта даних. Тому рекомендується збирати відповідну документацію із цього приводу, відповідно до раніше зазначених загальних правил щодо підтвердження фізичної особи, яка подає запит, і, якщо контролер має обґрунтовані сумніви щодо особи, яка діє від імені суб'єкта даних, він повинен запросити додаткову інформацію для підтвердження цієї особи.

82. Хоча реалізація права на доступ до персональних даних померлих осіб є ще одним прикладом доступу третьої сторони, відмінної від суб'єкта даних, преамбула 27 уточнює, що GDPR не застосовується до персональних даних померлих осіб. Таким чином, це питання регулюється національним законодавством, і держави-члени можуть передбачити правила щодо обробки персональних даних померлих осіб. Однак слід мати на увазі, що дані можуть, крім того, стосуватися живих третіх осіб, наприклад, у контексті запиту на отримання доступу до кореспонденції померлої особи. Конфіденційність таких даних все ще потребує захисту.

3.4.1 Здійснення права на доступ від імені дітей

83. Діти заслуговують на особливий захист щодо їхніх персональних даних, оскільки вони можуть бути менш обізнані про ризики, наслідки та гарантії, що стосуються їхніх прав у зв'язку з обробкою персональних даних [42] . Будь-яка інформація та спілкування з дитиною, де обробляються її персональні дані, має бути викладена чіткою та зрозумілою мовою, щоб дитина могла легко її зрозуміти[43].

84. Діти є суб'єктами персональних даних, а отже, право на доступ до них належить дитині. Залежно від зрілості та дієздатності дитини, їй може знадобитися третя сторона, яка діятиме від її імені, наприклад, особа, яка виконує батьківські обов'язки.

---

[41] Стаття 4(12) GDPR.

[42] Преамбула 38 GDPR. Як передбачено робочою програмою EDPB, вона має намір розробити настанови щодо даних про дітей. Очікується, що такий документ надасть більше вказівок щодо умов, за яких дитина може здійснювати своє право на доступ, а особа, яка несе батьківську відповідальність, може здійснювати право на доступ від імені дитини.

[43] Преамбула 58 GDPR. Настанови EDPB 05/2020 щодо надання згоди відповідно до Регламенту 2016/679, розділ 7.

85. Найкращі інтереси дитини повинні бути головним міркуванням у всіх рішеннях, що приймаються стосовно здійснення права на доступ до інформації в контексті дітей, зокрема, коли право на доступ здійснюється від імені дитини, наприклад, особою, яка має батьківські повноваження.

86. У зв'язку з особливим захистом персональних даних дітей, що міститься в GDPR, контролер повинен вжити належних заходів для уникнення будь-якого розкриття персональних даних неповнолітньої особи неуповноваженій особі (у зв'язку з цим див. також розділ 3.4 вище).

87. Зрештою, право особи, яка несе батьківську відповідальність, діяти від імені дитини не слід плутати з випадками, що виходять за рамки закону про захист даних, коли національне законодавство може передбачати право особи, яка несе батьківську відповідальність, запитувати та отримувати інформацію про дитину (наприклад, про успішність дитини в школі).

3.4.2 Реалізація права на доступ через портали/канали, надані третьою стороною

88. Існують компанії, які надають послуги, що дозволяють суб'єктам даних подавати запити на отримання доступу через портал. Суб'єкт даних реєструється та отримує доступ до порталу, через який він може подати, наприклад, запит на отримання доступу, запит на виправлення або видалення даних від різних контролерів. Різні питання виникають у зв'язку з використанням порталів, наданих третьою стороною.

89. Перше питання, яке необхідно вирішити контролерам, коли вони стикаються із цими обставинами, — це переконатися, що третя сторона діє на законних підставах від імені суб'єкта даних, оскільки необхідно переконатися, що жодні дані не будуть розкриті несанкціонованим особам.

90. Крім того, контролер, який отримує запит, зроблений через такий портал, завжди повинен своєчасно обробити цей запит[44]. Однак контролер не зобов'язаний надавати дані, передбачені статтею 15 GDPR, безпосередньо порталу, якщо контролер, наприклад, встановить, що заходи безпеки є недостатніми або вважатиме за доцільне використовувати інший спосіб розкриття даних суб'єкту даних. За таких обставин, якщо контролер має інші процедури для ефективної та безпечної обробки запитів на отримання доступу, він може надати запитувану інформацію за допомогою цих процедур.

4 ОБСЯГ ПРАВА НА ДОСТУП ТА ПЕРСОНАЛЬНІ ДАНІ ТА ІНФОРМАЦІЯ, НА ЯКІ ВОНО ПОШИРЮЄТЬСЯ

91. Цей розділ має на меті пролити світло на визначення персональних даних (4.1) та уточнити обсяг інформації, що охоплюється правом на доступ у цілому (4.2 та 4.3). Слід зазначити, що обсяг поняття персональних даних і, таким чином, розмежування між персональними даними та

[44] Щодо строків реалізації права на доступ, коли контролеру необхідно отримати додаткову інформацію, див. п. 157

іншими даними є невід'ємною частиною оцінки, що проводиться контролером для визначення обсягу даних, до яких суб'єкт даних має право отримати доступ[45].

92. Попередньо слід нагадати, що право на доступ може бути реалізоване лише щодо обробки персональних даних, які підпадають під матеріальну та територіальну сферу дії GDPR. Таким чином, персональні дані, які не обробляються автоматизованими засобами або які не є частиною або не призначені для того, щоб стати частиною системи реєстрації відповідно до статті 2(1) GDPR, або обробляються фізичною особою під час суто особистої або домашньої діяльності відповідно до статті 2(2) GDPR, не охоплюються правом на доступ.

4.1 Визначення персональних даних

93. Стаття 15(1) та (3) GDPR посилається на *«персональні дані»* та *«персональні дані, що підлягають обробці»*, відповідно. Таким чином, обсяг права на доступ визначається насамперед обсягом поняття персональних даних, визначеним у статті 4(1) GDPR[46]. Поняття персональних даних вже було предметом кількох документів[47] Робочої групи за статтею 29[48] та було витлумачено Судом ЄС, у тому числі в контексті права на доступ відповідно до статті 12 Директиви 95/46/ЄС.

94. Робоча група за статтею 29 вважала, що визначення персональних даних у Директиві 95/46/ЄС *«відображає намір європейського законодавця щодо широкого поняття «персональні дані»*[49]. Відповідно до GDPR, визначення все ще стосується *«будь-якої інформації, що стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи».* Окрім основних персональних даних, таких як ім'я та адреса, номер телефону тощо, під це визначення може підпадати необмежена кількість різноманітних даних, включаючи медичні висновки, історію покупок, показники кредитоспроможності, зміст повідомлень тощо. З огляду на широку сферу застосування визначення персональних даних, обмежувальна оцінка цього визначення

---

[45] Відповідно до принципу конфіденційності за задумом, такий аналіз є частиною оцінки належних заходів та гарантій захисту принципів захисту даних та прав суб'єктів даних, яка проводиться *«під час визначення засобів для обробки та під час самої обробки, наприклад,* скорочення часу відповіді, коли суб'єкти даних реалізують свої права, може бути одним із показників. Для подальших пояснень див. Настанови 4/2019 щодо статті 25 «Захист даних за задумом і за замовчуванням».

[46] Відповідно до статті 4(1) GDPR, «персональні дані» означають будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи»;

[47] Наприклад, РД 251, версія 01, Настанови щодо автоматизованого прийняття індивідуальних рішень та профайлінгу для цілей Регламенту 2016/679, тобто, с. 19; Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 9.

[48] Робоча група за статтею 29 — це незалежна європейська робоча група, яка займалася питаннями, пов'язаними із захистом приватності та персональних даних до 25 травня 2018 року (вступу в дію GDPR), попередник EDPB.

[49] Висновок 4/2007 Робочої групи за статтею 29 щодо поняття персональних даних, с. 4.

контролером призведе до помилкової класифікації персональних даних [50] і, в кінцевому підсумку, до порушення права на доступ до них.

95. В об'єднаних справах C-141/12 та C-372/12[51] Суд ЄС постановив, що право на доступ поширюється на персональні дані, що містяться в протоколах, а саме *«ім'я, дату народження, громадянство, стать, етнічну приналежність, релігію та мову заявника» «та, за необхідності, на дані правового аналізу, що містяться в протоколі»*, але не на сам правовий аналіз[52]. У цьому контексті правовий аналіз сам по собі не підлягав перевірці його точності суб'єктом даних і не підлягав виправленню. Крім того, надання доступу до правового аналізу не відповідає меті гарантування приватності, а є доступом до адміністративних документів.

96. У справі «Новак»[53] Суд ЄС здійснив ширший аналіз і встановив, що письмові відповіді, надані кандидатом на професійному іспиті, та будь-які коментарі екзаменатора щодо цих відповідей становлять персональні дані, що стосуються кандидата на іспиті. Точніше, така суб'єктивна інформація є персональними даними *«у формі думок та оцінок, за умови, що вона «стосується» суб'єкта даних»*[54], на відміну від екзаменаційних питань, які не вважаються персональними даними[55]. Таким чином, контекстуальна оцінка повинна пролити світло на вплив або результат, який інформація може мати на особу, а отже, і на обсяг права на доступ.

> **Приклад 15:** Особа проходить співбесіду з компанією. У цьому контексті кандидат на роботу подає резюме та лист-заяву. Під час співбесіди працівник відділу кадрів робить нотатки на комп'ютері, щоб задокументувати співбесіду. Після цього кандидат на посаду як суб'єкт даних запитує доступ до персональних даних, що його стосуються, які компанія, як контролер, зібрала під час процедури набору персоналу.
>
> Контролер зобов'язаний надати суб'єкту персональних даних персональні дані, які він активно повідомляв у своєму резюме та заяві. Крім того, контролер повинен надати суб'єкту даних резюме співбесіди, включаючи суб'єктивні коментарі щодо поведінки суб'єкта даних, які співробітник відділу кадрів написав під час співбесіди, з урахуванням будь-яких винятків, передбачених національним законодавством, і відповідно до статті 23 GDPR.

97. Таким чином, залежно від конкретних фактів справи, при оцінці конкретного запиту на отримання доступу, контролери, *серед іншого,* повинні надавати наступні типи даних, не обмежуючи змісту статті 15(4) GDPR:

---

[50] Як інформації, що не стосується ідентифікованої фізичної особи або такої, що може бути ідентифікована.

[51] Суд ЄС, об'єднані справи C-141/12 та C-372/12, YS проти Міністра з питань імміграції, інтеграції та асиміляції та Міністра з питань імміграції, інтеграції та асиміляції проти M та S, 17 липня 2014 року.

[52] Суд ЄС, об'єднані справи C-141/12 та C-372/12, YS та інші, п. 38 і 48.

[53] Суд ЄС, C-434/16, «Пітер Новак проти Комісара з питань захисту даних», 20 грудня 2017 року.

[54] Суд ЄС, C 434/16, «Новак», п. 34-35.

[55] Суд ЄС, C-434/16, «Новак», п. 58.

- спеціальні категорії персональних даних відповідно до статті 9 GDPR;
- персональні дані, що стосуються кримінальних судимостей та правопорушень, відповідно до статті 10 GDPR;
- дані, свідомо та активно надані суб'єктом даних (наприклад, дані облікового запису, надані через форми, відповіді на анкети)[56];
- дані спостережень або необроблені дані, надані суб'єктом даних внаслідок використання послуги або пристрою (наприклад, дані, оброблені підключеними об'єктами, історія транзакцій, журнали активності, такі як журнали доступу, історія використання вебсайту, пошукова активність, дані про місцезнаходження, активність кліків, унікальні аспекти поведінки людини, такі як почерк, натискання клавіш, особлива манера ходити або говорити)[57];
- дані, отримані з інших даних, а не безпосередньо надані суб'єктом даних (наприклад, кредитний коефіцієнт, класифікація на основі загальних атрибутів суб'єктів даних, країна проживання на основі поштового індексу)[58];
- дані, виведені з інших даних, а не безпосередньо надані суб'єктом даних (наприклад, для присвоєння кредитного рейтингу або дотримання правил боротьби з відмиванням грошей, алгоритмічні результати, результати оцінки стану здоров'я або процесу персоналізації чи надання рекомендацій)[59];
- псевдонімізовані дані на відміну від знеособлених даних (див. також розділ 3 цих настанов).

[56] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 9.

[57] Висновок 4/2007 Робочої групи за статтею 29 щодо поняття персональних даних, с. 8

[58] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 10-11

[59] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 10-11; Робоча група за статтею 29, РД 251, версія 01, 6 лютого 2018 року, Настанови щодо автоматизованого прийняття індивідуальних рішень та профайлінгу для цілей Регламенту 2016/679 – схвалені EDPB (далі — «Настанови Робочої групи за статтею 29 щодо автоматизованого прийняття індивідуальних рішень та профайлінгу – схвалені EDPB»), с. 9-10.

Приклад 16: Аспекти, які були використані для прийняття рішення, зокрема про просування працівника по службі, підвищення заробітної плати або призначення на нову роботу (наприклад, щорічні оцінки результатів діяльності, запити на навчання, дисциплінарні записи, рейтинг, кар'єрний потенціал), є персональними даними, що стосуються цього працівника. Таким чином, суб'єкт даних може отримати доступ до таких аспектів за запитом і з дотриманням статті 15(4) GDPR, якщо персональні дані також стосуються іншої особи (наприклад, особа або аспекти, що розкривають особу іншого працівника, чиї свідчення про професійну діяльність включені до щорічної оцінки ефективності, можуть підлягати обмеженням відповідно до статті 15(4) GDPR), а отже, можливо, вони не можуть бути повідомлені суб'єкту даних з метою захисту прав і свобод цього працівника). Однак можуть застосовуватися положення національного трудового законодавства, наприклад, щодо доступу працівників до особових справ, або інші національні положення, зокрема щодо професійної таємниці. За будь-яких обставин, такі обмеження на здійснення права на доступ суб'єкта даних (або інших прав), передбачені національним законодавством, повинні відповідати умовам статті 23 GDPR (див. розділ 6.4).

98. З наведеного вище невичерпного переліку персональних даних, які можуть бути надані суб'єкту даних у контексті запиту на отримання доступу, можна зробити кілька висновків. З наведеного вище випливає, що при наданні доступу до персональних даних контролер може не робити різниці між даними, що містяться в паперових файлах, і тими, що зберігаються в електронному вигляді, якщо вони підпадають під дію GDPR. Іншими словами, на персональні дані, які містяться в паперових файлах як частина картотеки або призначені для того, щоб стати частиною картотеки, поширюється право на доступ, так само як і на персональні дані, що зберігаються в пам'яті комп'ютера за допомогою, наприклад, двійкового коду або відеокасети.

99. Крім того, як і більшість прав суб'єкта даних, право на доступ включає як похідні, так і виведені дані, в тому числі персональні дані, створені постачальником послуг, тоді як право на перенесення даних включає лише дані, надані суб'єктом даних[60]. Таким чином, у випадку запиту на отримання доступу, на відміну від запиту на перенесення даних, суб'єкту даних мають бути надані не лише персональні дані, надані контролеру з метою проведення подальшого аналізу чи оцінки цих даних, але й результат будь-якого такого подальшого аналізу чи оцінки.

100. Важливо також нагадати, що існує така інформація, як знеособлені дані[61], тобто дані, які прямо чи опосередковано не стосуються особи, яку можна ідентифікувати, і які, таким чином, виключаються зі сфери дії GDPR. Наприклад, місцезнаходження сервера, на якому обробляються персональні дані суб'єкта даних, не є персональними даними. Розмежування може бути складним, і контролери можуть задатися питанням, як провести чітку межу між персональними та неперсональними даними, особливо у випадку змішаних наборів даних. У такому випадку

[60] Як зазначалося раніше в Настановах Робочої групи за статтею 29 щодо права на перенесення даних, схвалених EDPB, п. 10, і підтверджено в Настановах Робочої групи за статтею 29 щодо автоматизованого прийняття індивідуальних рішень та профайлінгу, схвалених EDPB, п. 17.

[61] Подальші пояснення щодо поняття знеособлення можна знайти у Висновку 05/2014 Робочої групи за статтею 29 щодо методів знеособлення, РД 216, 10 квітня 2014 року, с. 5-19.

може бути корисним розрізняти змішані набори даних, у яких персональні та неперсональні дані нерозривно пов'язані, і ті, в яких це не так. Персональні та неперсональні дані можуть бути нерозривно пов'язані в змішаних наборах даних і повністю підпадати під сферу дії права на доступ суб'єкта даних, якого стосуються персональні дані[62]. В інших випадках персональні та неперсональні дані в змішаних наборах даних можуть не бути нерозривно пов'язані, внаслідок чого суб'єкт даних може мати доступ лише до персональних даних у наборі. Наприклад, компанії може знадобитися надати суб'єкту даних окремі звіти про IT-інциденти, які він спровокував, але не базу знань компанії про IT-проблеми. Однак, заходи безпеки, які вжив контролер, як правило, не слід розуміти як персональні дані, якщо вони не є нерозривно пов'язаними з персональними даними, а отже, не підпадають під дію права на доступ до них.

101. Перш ніж завершити розділ, EDPB нагадує в цьому контексті, що захист фізичних осіб у зв'язку з обробкою персональних даних охоплює всі види персональних даних, перелічені вище, і що обмежувальне тлумачення цього визначення суперечить положенням GDPR і, зрештою, порушує статтю 8 Хартії основоположних прав людини. Застосування іншого режиму реалізації права щодо деяких видів персональних даних, який не був передбачений GDPR, може бути запроваджений виключно законом, відповідно до статті 23 GDPR (як далі пояснюється в розділі 6.4). Таким чином, контролери не можуть обмежувати реалізацію права на доступ шляхом неправомірного обмеження обсягу персональних даних.

4.2 Персональні дані, на які поширюється право на доступ

102. Відповідно до статті 15(1) GDPR, *«суб'єкт даних має право отримати від контролера підтвердження того, чи обробляються його персональні дані, і, якщо це так, доступ до персональних даних та наступної інформації» (виділено* нами).

103. З пункту (1) статті 15 GDPR випливає кілька аспектів. Цей пункт *прямо посилається* на *«персональні дані, що його стосуються»* (4.2.1), які *«обробляються»* (4.2.2) контролером:

4.2.1 «персональні дані, що його стосуються»

104. Право на доступ може бути реалізоване виключно щодо персональних даних, які стосуються суб'єкта даних, який запитує доступ, або, у відповідних випадках, уповноваженою особою чи довіреною особою (див. розділ 3.4). Існують також ситуації, коли дані пов'язані не з особою, яка здійснює право на доступ, а з іншою особою. Однак суб'єкт даних має право лише на персональні дані, що стосуються його самого, за винятком даних, які стосуються виключно іншої особи[63].

---

[62] Повідомлення Комісії Європейському Парламенту та Раді, Настанови щодо Регламенту про рамки для вільного руху неперсональних даних у Європейському Союзі, 29.05.2019 р., Повідомлення 2019/250, фінальна версія.

[63] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, с. 9: *«Запит на перенесення даних стосується лише персональних даних. Таким чином, будь-які знеособлені дані або дані, що не стосуються суб'єкта даних, не підпадають під сферу дії запиту. Однак псевдонімні дані, які можна чітко пов'язати із суб'єктом даних (наприклад, шляхом надання ним відповідного ідентифікатора, див. статтю 11(2)), входять до сфери його дії».*

105. Класифікація даних як персональних даних, що стосуються суб'єкта даних, не залежить, однак, від того, що ці персональні дані також стосуються іншої особи[64]. Таким чином, можлива ситуація, коли персональні дані стосуються більше ніж однієї особи одночасно. Це не означає автоматичного надання доступу до персональних даних, які також стосуються іншої особи, оскільки контролер повинен дотримуватися вимог статті 15(4) GDPR.

106. Слова *«персональні дані, що його стосуються»* не повинні тлумачитися контролерами в *«надмірно обмежувальний»* спосіб, як вже зазначалося Робочою групою за статтею 29 щодо права на перенесення даних[65]. Стосовно права на доступ, EDPB вважає, що, наприклад, записи телефонних розмов (та їх транскрипція) між суб'єктом даних, який запитує доступ, та контролером, можуть підпадати під право на доступ за умови, що останні є персональними даними[66]. За умови, що застосовується GDPR і що обробка не підпадає під виняток для домогосподарств відповідно до статті 2(2)(c), якщо суб'єкт даних використовує отриманий запис, який містить персональні дані співрозмовника, для інших цілей, наприклад, публікуючи запис, суб'єкт даних стає контролером цієї обробки персональних даних, що стосуються іншої особи, чий голос був записаний. Хоча це не звільняє контролера від його зобов'язань щодо захисту даних при належному аналізі можливості надання доступу до повного запису, контролеру рекомендується інформувати суб'єкта даних про те, що він може стати контролером у такому випадку. Це не впливає на будь-яку подальшу оцінку відповідно до статті 15(4) GDPR, детально описану в розділі 6. Так само повідомлення, які суб'єкти даних надіслали іншим особам у вигляді міжособистісних повідомлень і видалили зі свого пристрою, але які все ще доступні для постачальника послуг, можуть підпадати під право на доступ.

107. З іншого боку, існують ситуації, у яких зв'язок між даними та кількома особами може здаватися контролеру розмитим, як, наприклад, у випадку крадіжки персональних даних. У випадку крадіжки персональних даних особа шахрайським шляхом діє від імені іншої особи. У цьому контексті важливо нагадати, що потерпілому має бути надана інформація про всі персональні дані, які контролер зберігає у зв'язку з його особою, включаючи ті, які були зібрані на підставі дій шахрая. Іншими словами, навіть після того, як контролер дізнався про крадіжку персональних

---

[64] Суд ЄС, рішення у справі C-434/16 «Пітер Новак проти Комісара з питань захисту даних», 2017, п. 44.

[65] Настанови Робочої групи за статтею 29 щодо права на перенесення даних – схвалені EDPB, п. 9: *За багатьох обставин контролери обробляють інформацію, яка містить персональні дані кількох суб'єктів даних. У таких випадках контролери не повинні надмірно обмежувати тлумачення фрази «персональні дані, що стосуються суб'єкта даних». Наприклад, записи телефонних розмов, міжособистісних повідомлень або VoIP можуть містити (в історії облікового запису абонента) інформацію про третіх осіб, які брали участь у вхідних та вихідних дзвінках. Хоча записи, таким чином, будуть містити персональні дані, що стосуються кількох осіб, абоненти повинні мати можливість отримати ці записи у відповідь на запит про перенесення даних, оскільки ці записи (також) стосуються суб'єкта даних. Однак, якщо такі записи потім передаються новому контролеру, цей новий контролер не повинен обробляти їх з будь-якою метою, яка може негативно вплинути на права та свободи третіх осіб (див. нижче: третя умова)».*

[66] Див. приклад 34 у розділі 6.2.

даних, персональні дані, які пов'язані або стосуються особи потерпілого, є персональними даними суб'єкта даних.

Приклад 17: Фізична особа шахрайським шляхом використовує чужі персональні дані для гри в покер в Інтернеті. Зловмисник розплачується з онлайн-казино кредитною карткою, яку він викрав у жертви. Коли жертва дізнається про крадіжку персональних даних, вона просить провайдера онлайн-казино надати їй доступ до своїх персональних даних, зокрема, до зіграних онлайн-ігор та інформації про кредитну картку, яку використовував злочинець.

Існує зв'язок між зібраними даними та жертвою, оскільки було використано її персональні дані. Після виявлення шахрайства згадані вище персональні дані все ще мають зв'язок через їхній зміст (кредитна картка жертви явно стосується жертви), мету та наслідки (інформація про онлайн-ігри, в які грав злочинець, може бути використана, наприклад, для виставлення рахунків жертві). Тому онлайн-казино має надати жертві доступ до вищезазначених персональних даних.

108. Якщо це доцільно, внутрішні журнали з'єднань можуть використовуватися для зберігання записів про доступ до файлу та для відстеження того, які дії були виконані у зв'язку з доступом до запису, наприклад, друк, копіювання або видалення персональних даних. Ці журнали можуть містити час реєстрації, причину доступу до файлу, а також інформацію, що ідентифікує особу, яка отримала доступ. Питання, пов'язані із цією темою, є предметом розгляду у справі, яка наразі перебуває на розгляді в Суді ЄС (C-579/21). Запровадження, нагляд і перегляд журналів з'єднань належать до обов'язків контролера та підлягають перевірці з боку наглядових органів. Таким чином, контролер повинен переконатися, що особи, які діють під його керівництвом і мають доступ до персональних даних, не обробляють персональні дані, крім як за вказівкою контролера, відповідно до статті 29 GDPR. Якщо особа все ж таки обробляє персональні дані для інших цілей, ніж виконання інструкцій контролера, вона може стати контролером цієї обробки та підлягати дисциплінарному чи кримінальному переслідуванню або адміністративним санкціям з боку наглядових органів. EDPB зазначає, що це частина відповідальності роботодавця відповідно до статті 24 GDPR вживати відповідних заходів, починаючи від навчання та закінчуючи дисциплінарними процедурами, для забезпечення того, щоб обробка відповідала вимогам GDPR і не допускала жодних порушень.

4.2.2 Персональні дані, які «обробляються»

109. Пункт (1) статті 15 GDPR, крім того, посилається на персональні дані, які «обробляються». Часовий орієнтир для визначення кола персональних даних, що підпадають під запит на отримання доступу, вже був розглянутий у розділі 2.3.3. Однак формулювання також свідчить про те, що право на доступ не робить різниці між цілями операцій з обробки.

Приклад 18: Компанія обробляла персональні дані, що стосуються суб'єкта даних, з метою обробки його замовлення на купівлю та організації доставки на домашню адресу суб'єкта даних. Після того, як ці початкові цілі, для яких збиралися персональні дані, більше не існують, контролер зберігає частину персональних даних виключно для виконання своїх юридичних зобов'язань, пов'язаних із веденням обліку.

Суб'єкт даних запитує доступ до персональних даних, які його стосуються. Щоб виконати свій обов'язок згідно зі статтею 15(1) GDPR, контролер повинен надати суб'єкту даних запитувані персональні дані, які зберігаються для виконання своїх юридичних зобов'язань.

110. Заархівовані персональні дані слід відрізняти від резервних даних, які є персональними даними, що зберігаються виключно з метою відновлення даних у випадку їх втрати. Слід зазначити, що з точки зору принципів захисту даних за призначенням та мінімізації даних, резервні дані в цілому подібні до даних у продуктивній системі. Якщо існують незначні відмінності між персональними даними в резервній копії та продуктивній системі, вони, як правило, пов'язані зі збором додаткових даних з моменту останнього резервного копіювання. Зменшення кількості даних у продуктивній системі (наприклад, видалення після закінчення терміну зберігання деяких даних або після запиту на видалення) в деяких випадках буде перезаписано в резервну копію даних лише під час наступного резервного копіювання. У разі надходження запиту на отримання доступу у момент, коли в резервній копії міститься більше персональних даних, що стосуються суб'єкта даних, ніж у продуктивній системі, або коли персональні дані відрізняються (що можна помітити, наприклад, за допомогою журналу видалень у продуктивній системі, реалізованій у повній відповідності до принципу мінімізації даних), контролер повинен бути прозорим щодо цієї ситуації та, якщо це технічно можливо, надати доступ на вимогу суб'єкта даних, у тому числі до персональних даних, що зберігаються в резервній копії. Наприклад, з метою забезпечення прозорості для суб'єктів даних, які реалізують своє право, журнал видалень у продуктивній системі може дозволити контролеру побачити, що в резервній копії є дані, яких більше немає в продуктивній системі, оскільки вони були нещодавно видалені й ще не були перезаписані в резервну копію.

4.2.3 Обсяг нового запиту на отримання доступу

111. Залишається сказати, що суб'єкти даних мають право на доступ до всіх оброблених даних, що стосуються їх, або до частини даних, залежно від обсягу запиту (див. також розділ 2.3.1 про повноту інформації та розділ 3.1.1 про аналіз змісту запиту). Як наслідок, якщо контролер вже задовольнив запит на отримання доступу до інформації в минулому та за умови, що запит не є надмірним, контролер не може звузити обсяг цього нового запиту. Це означає, що у зв'язку з будь-яким наступним запитом на отримання доступу того самого суб'єкта даних контролер не повинен інформувати суб'єкта даних лише про зміни в оброблених персональних даних або в самій обробці з моменту останнього запиту, якщо тільки суб'єкт даних не висловив на це свою явну згоду. В іншому випадку суб'єкти даних будуть зобов'язані зібрати надані ними персональні дані для того, щоб отримати повний набір персональних даних, що стосуються їхньої інформації про обробку та права суб'єктів даних.

4.3 Інформація про обробку та права суб'єктів даних

112. Окрім доступу до самих персональних даних, контролер повинен надати інформацію про обробку та права суб'єктів даних відповідно до статті 15(1)(a)-(h) та 15(2) GDPR. Більшість інформації із цих конкретних питань вже зібрана, принаймні в загальній формі, у записі контролера про діяльність з обробки, зазначеній у статті 30 GDPR, та/або в його повідомленні про конфіденційність, розробленому відповідно до статей 12-14 GDPR. Тому першим кроком може бути корисно ознайомитися з «Настановами щодо прозорості відповідно до Регламенту

2016/679»[67] Робочої групи за статтею 29 щодо змісту інформації, яку слід надавати відповідно до статей 13 та 14 GDPR.

113. Для того, щоб відповідати вимогам статті 15(1)(a)-(h) та 15(2), контролери можуть обережно використовувати текстові модулі своїх повідомлень про конфіденційність, якщо вони переконаються, що вони є актуальними й точними щодо запиту суб'єкта даних. До або на початку обробки даних певна інформація, наприклад, ідентифікація конкретних одержувачів або конкретна тривалість обробки даних, часто ще не може бути надана. Деяка інформація, як-от право на подання скарги до наглядового органу (див. статтю 15(1)(f)), не змінюється залежно від того, хто подає запит на отримання доступу до даних, тому вона може бути повідомлена в загальних рисах, як це також робиться в повідомленні про конфіденційність. Інші види інформації, такі як інформація про одержувачів, категорії та джерело даних, можуть відрізнятися залежно від того, хто подає запит і який обсяг запиту. У контексті запиту на отримання доступу відповідно до статті 15, будь-яка інформація про обробку, наявна у контролера, може бути оновлена та адаптована до операцій з обробки, що фактично здійснюються щодо суб'єкта даних, який подає запит. Таким чином, посилання на формулювання своєї політики конфіденційності не буде достатнім для того, щоб контролер надав інформацію, яка вимагається за статтею 15(1)(a)-(h) та (2), якщо тільки «адаптована та оновлена» інформація не є такою ж, як інформація, надана на початку обробки. Пояснюючи, яка інформація стосується особи, що подала запит, контролер може, за необхідності, посилатися на певні дії (наприклад, «якщо ви користувалися цією послугою...», «якщо ви заплатили за рахунком»), якщо це очевидно для суб'єктів даних, якщо їх це стосується. Далі пояснюється ступінь необхідної конкретизації щодо окремих типів інформації.

114. Інформація про мету відповідно до статті 15(1)(a) повинна бути конкретною щодо точної мети (цілей) у конкретному випадку суб'єкта даних, який подає запит. Недостатньо перерахувати загальні цілі контролера, не уточнивши, яку саме мету контролер переслідує у конкретній справі суб'єкта даних, який подав запит. Якщо обробка здійснюється з кількома цілями, контролер повинен пояснити, які дані або які категорії даних обробляються з якою метою (цілями). На відміну від статті 13(1)(c) та статті 14(1)(c) GDPR, інформація про обробку, зазначена в статті 15(1)(a), не містить інформації про законну підставу для обробки. Однак, оскільки деякі права суб'єктів даних залежать від застосовної законної підстави, ця інформація важлива для суб'єктів даних, щоб перевірити законність обробки даних та визначити, які права суб'єкта даних застосовуються в конкретній ситуації. Тому, щоб полегшити суб'єктам даних реалізацію їхніх прав відповідно до статті 12(2) GDPR, контролеру рекомендується також інформувати суб'єкта даних про застосовну законну підставу для кожної операції з обробки або вказувати, де він може знайти цю інформацію. У будь-якому випадку, принцип прозорої обробки вимагає, щоб інформація про правові підстави обробки була надана суб'єкту даних у доступній формі (наприклад, у повідомленні про конфіденційність).

[67] Настанови щодо прозорості відповідно до Регламенту 2016/679 – схвалені EDPB (далі — «Настанови Робочої групи за статтею 29 щодо прозорості – схвалені EDPB») Робочої групи за статтею 29, РД 260, версія 01, 11 квітня 2018 року.

115. Інформація про категорії даних (стаття 15(1)(b)) також може бути адаптована до ситуації суб'єкта даних таким чином, що категорії, які виявилися нерелевантними для запитувача, повинні бути виключені.

> **Приклад 19**: У контексті інформації, зазначеної в статті 13/14 GDPR, готель заявляє, що обробляє низку категорій даних клієнтів (ідентифікаційні дані, контактні дані, банківські дані, номер кредитної картки тощо). Якщо запит на отримання доступу подається на підставі статті 15, то суб'єкт даних, який подає запит, повинен, окрім доступу до фактичних даних, що обробляються (компонент 2), відповідно до статті 15(1)(b), також бути поінформованим про конкретні категорії даних, які обробляються в конкретному випадку (наприклад, не включати банківські дані або дані кредитної картки, якщо оплата була здійснена готівкою).

116. Інформація про «одержувачів або категорії одержувачів» (стаття 15(1)(c)) повинна, перш за все, враховувати визначення одержувачів, наведене в статті 4(9) GDPR. Визначення одержувачів ґрунтується на розкритті персональних даних фізичній або юридичній особі, органу державної влади, агентству або іншому органу[68]. Зі змісту статті 4(9) GDPR випливає, що органи державної влади, які діють у рамках конкретного запиту відповідно до конкретних національних положень, не вважаються одержувачами.

117. Щодо питання, чи може контролер вільно вибирати між інформацією про одержувачів або про категорії одержувачів, слід зазначити, що «на відміну від статей 13 і 14 GDPR, які встановлюють обов'язок контролера (...), стаття 15 GDPR встановлює реальне право суб'єкта даних, у результаті чого суб'єкт даних має можливість отримати або інформацію про конкретних одержувачів, яким дані були або будуть розкриті, за можливості, або інформацію про категорії одержувачів».[69] Слід також нагадати, що, як зазначено у вищезгаданих настановах щодо прозорості[70], вже відповідно до статей 13 і 14 GDPR інформація про одержувачів або категорії одержувачів повинна бути максимально конкретною з точки зору принципів прозорості та справедливості. Відповідно до статті 15, якщо суб'єкт даних не вибрав іншого, контролер зобов'язаний назвати фактичних одержувачів, якщо тільки неможливо ідентифікувати цих одержувачів або контролер не доведе, що запити суб'єкта даних на отримання доступу є явно необґрунтованими або надмірними в розумінні статті 12(5) GDPR[71][72]. У зв'язку із цим EDPB нагадує, що зберігання інформації, що

---

[68] Слід також зазначити, що різні контролери, визначені статтею 4(7) GDPR, можуть існувати в межах однієї компанії. У цьому випадку можливе розкриття даних від одного одержувача до іншого в межах однієї компанії.

[69] Суд ЄС, C-154/21 (Osterreichische Post AG), п. 36.

[70] Настанови щодо прозорості відповідно до Регламенту 2016/679 – схвалені EDPB (далі — «Настанови Робочої групи за статтею 29 щодо прозорості – схвалені EDPB») Робочої групи за статтею 29, РД 260, версія 01, 11 квітня 2018 року, п. 37 (Додаток)

[71] Суд ЄС, C-154/21 (Österreichische Post AG)

[72] Факт розкриття даних великій кількості одержувачів *сам по собі* не робить запит надмірним (див. розділ 6, п. 188).

стосується фактичних одержувачів, необхідне, *серед іншого*, для того, щоб мати можливість виконувати зобов'язання контролера відповідно до статей 5(2) і 19 GDPR.

Приклад 20: У своєму повідомленні про конфіденційність роботодавець надає інформацію про те, які категорії даних передаються «туристичним агентствам» або «готелям» у разі відряджень, відповідно до статей 13(1)(e) та 14(1)(e) GDPR. Якщо працівник подає запит на отримання доступу до персональних даних після завершення відрядження, роботодавець повинен вказати одержувачів персональних даних відповідно до статті 15(1)(c), у своїй відповіді вказати туристичне(-і) агентство(-а) та готель(-і), які отримали ці дані. Хоча роботодавець законно вказав категорії одержувачів у своєму повідомленні про конфіденційність відповідно до статей 13 і 14, оскільки на цьому етапі ще не було можливості назвати одержувачів, він повинен, якщо працівник не вирішив інакше, надати інформацію про конкретних одержувачів (назви туристичних агентств, готелів тощо), коли працівник подає запит на отримання доступу до даних.

Якщо, дотримуючись вищезазначених умов, контролер може надати лише категорії одержувачів, інформація повинна бути максимально конкретною, із зазначенням типу одержувача (тобто з посиланням на діяльність, яку він здійснює), галузі, сектору та підсектору, а також місцезнаходження одержувачів[73].

118. Відповідно до статті 15(1)(d), якщо це можливо, необхідно надати інформацію про передбачуваний період, протягом якого персональні дані будуть зберігатися. В іншому випадку, повинні бути надані критерії, що використовуються для визначення цього періоду. Інформація, надана контролером, повинна бути достатньо точною, щоб суб'єкт даних знав, як довго будуть зберігатися дані, що стосуються суб'єкта даних. Якщо неможливо вказати час видалення, необхідно вказати тривалість періодів зберігання та початок цього періоду або подію, що його ініціює (наприклад, розірвання договору, закінчення гарантійного терміну тощо). Простого посилання, наприклад, на «видалення після закінчення встановлених законом термінів зберігання» недостатньо. Вказівки щодо термінів зберігання даних повинні бути зосереджені на конкретних даних, що стосуються суб'єкта даних. Якщо персональні дані суб'єкта даних підлягають різним термінам видалення (наприклад, тому що не на всі дані поширюються юридичні зобов'язання щодо зберігання), терміни видалення повинні бути зазначені стосовно відповідних операцій з обробки та категорій даних.

119. У той час як інформація про право подати скаргу до наглядового органу (стаття 15(1)(f)) не залежить від конкретних обставин, права суб'єктів даних, зазначені в статті 15(1)(e), варіюються залежно від законної підстави, на якій ґрунтується обробка. Що стосується зобов'язання сприяти здійсненню прав суб'єктів даних відповідно до статті 12(2) GDPR, то відповідь контролера щодо цих прав повинна бути індивідуально адаптована до випадку суб'єкта даних і стосуватися відповідних операцій з обробки. Слід уникати інформації про права, які не застосовуються до суб'єкта даних у конкретній ситуації.

[73] Настанови Робочої групи за статтею 29 щодо прозорості – схвалені EDPB, с. 37 (Додаток)

120. Відповідно до статті 15(1)(g), «будь-яка доступна інформація» про джерело даних повинна бути надана, якщо персональні дані не збираються від суб'єкта даних. Обсяг доступної інформації може змінюватися з часом.

> **Приклад 21**: У політиці конфіденційності великої компанії зазначено:
>
> «Кредитні перевірки допомагають нам запобігти проблемам у платіжних операціях. Вони гарантують захист нашої компанії від фінансових ризиків, які також можуть вплинути на ціни продажу в середньостроковій і довгостроковій перспективі. Кредитна перевірка обов'язково проводиться, коли ми збираємося відвантажити товар без одночасного отримання відповідної ціни придбання, наприклад, у випадку купівлі на умовах передоплати. Без проведення перевірки кредитоспроможності можливий лише варіант передоплати (негайний банківський переказ, платіжна система, кредитна картка).
>
> З метою перевірки кредитоспроможності ми надішлемо ваше ім'я, адресу та дату народження таким постачальникам послуг, наприклад: (1) Агентство фінансової інформації X, (2) Постачальник ділової інформації Y, (3) Комерційне бюро кредитних історій Z.
>
> Дані передаються вищезазначеним кредитним установам лише в межах, дозволених законом, і лише з метою аналізу вашої минулої платіжної поведінки, а також для оцінки ризику невиконання зобов'язань на основі математично-статистичних процедур з використанням адресних даних, а також для перевірки вашої адреси (перевірки доставки). Залежно від результату перевірки кредитоспроможності, ми, можливо, більше не зможемо запропонувати вам індивідуальні способи оплати, такі як купівля рахунків-фактур».
>
> Таким чином, повідомлення про конфіденційність містить загальну інформацію про можливість отримання інформації від перелічених бюро економічної інформації відповідно до статей 13 і 14 GDPR. Якщо заздалегідь не зрозуміло, яка з компаній братиме участь в обробці, достатньо вказати в політиці конфіденційності назви відповідних компаній. У контексті запиту на підставі статті 15, на додаток до інформації про те, що інформація про кредитоспроможність була отримана, потім (ex post) необхідно буде розкрити інформацію про те, яка саме компанія була залучена до обробки. Це чітко визначено в статті 15(1)(g), що інформація про обробку даних включає «будь-яку наявну інформацію про їхнє джерело», якщо персональні дані не збираються від суб'єкта даних.

121. Стаття 15(1)(h) передбачає, що кожен суб'єкт даних повинен мати право бути поінформованим у належний спосіб, *серед іншого*, про існування та основну логіку автоматизованого прийняття рішень, включаючи профайлінг, щодо суб'єкта даних, а також про значення та передбачувані наслідки, які може мати така обробка [74]. Якщо це можливо, інформація, передбачена статтею 15(1)(h) повинна бути більш конкретною щодо аргументації, яка призвела до прийняття конкретних рішень стосовно суб'єкта даних, який звернувся з проханням про надання доступу.

[74] Див. із цього приводу Настанови щодо прозорості відповідно до Регламенту 2016/679 (РД 260), п. 41, з посиланням на Настанови щодо автоматизованого прийняття індивідуальних рішень та профайлінгу для цілей Регламенту 2016/679 (РД 251).

122. Інформація про заплановану передачу даних до третьої країни або міжнародної організації, включаючи наявність належного рішення або відповідних гарантій Комісії, повинна бути надана відповідно до статей 13(1)(f) та 14(1)(f) GDPR. У контексті запиту на отримання доступу відповідно до статті 15, пункт (2) статті 15 вимагає надання інформації про відповідні гарантії згідно зі статтею 46 GDPR лише у випадках, коли передача даних до третьої країни або міжнародної організації дійсно відбувається.

5 ЯК КОНТРОЛЕР МОЖЕ ЗАБЕЗПЕЧИТИ НАДАННЯ ДОСТУПУ?

123. GDPR не містить чітких вказівок щодо того, як контролер повинен надавати доступ. Право на доступ може бути простим і зрозумілим для застосування в деяких ситуаціях, наприклад, коли невелика організація має обмежену інформацію про суб'єкта даних. В інших ситуаціях право на доступ є більш складним, оскільки обробка даних є більш складною, що стосується кількості суб'єктів даних, категорій даних, що обробляються, а також потоку даних всередині та між різними організаціями. Враховуючи відмінності в обробці персональних даних, відповідний спосіб надання доступу може відрізнятися.

124. Цей розділ має на меті надати деякі вказівки та практичні приклади щодо різних способів виконання контролерами запиту на отримання доступу, а також значення статті 12(1) GDPR щодо надання доступу до персональних даних. Цей розділ також містить деякі вказівки щодо того, що вважається загальновживаною електронною формою, а також щодо термінів надання доступу відповідно до статті 12(3) GDPR.

5.1 Як контролер може отримати запитувані дані?

125. Суб'єкти даних повинні мати доступ до всієї інформації, яку обробляє про них контролер. Це означає, наприклад, що контролер зобов'язаний здійснювати пошук персональних даних у своїх IT-системах та не IT-системах реєстрації. Здійснюючи такий пошук, контролер повинен використовувати наявну в організації інформацію про суб'єкта даних, яка, ймовірно, призведе до збігів у системах залежно від того, як інформація структурована[75]. Наприклад, якщо інформація відсортована у файлах залежно від імені або реєстраційного номера, пошук може бути обмежений цими факторами. Але якщо структура даних залежить від інших факторів, таких як родинні зв'язки, професійні звання або будь-які прямі чи непрямі ідентифікатори (наприклад, номер клієнта, ім'я користувача або IP-адреса), пошук необхідно розширити, щоб включити їх, за умови, що контролер також володіє цією інформацією, пов'язаною із суб'єктом даних, або отримав цю інформацію від суб'єкта даних. Те саме стосується випадків, коли записи щодо третіх осіб можуть містити персональні дані суб'єкта даних. Однак контролер не може вимагати від суб'єкта даних надання більшого обсягу інформації, ніж це необхідно для ідентифікації суб'єкта даних. Якщо контролер використовує оператора для обробки даних, пошук, звичайно, повинен бути розширений, щоб також включати персональні дані, які обробляються оператором.

[75] Такий пошук зазвичай повинен також включати інформацію, яка зберігається у процесора, див. статтю 28(3)(e) GDPR.

126. Відповідно до статті 25 GDPR про захист даних за призначенням і за замовчуванням, контролер (і будь-які оператори, яких він використовує) також повинен вже мати реалізовані функції, що забезпечують дотримання прав суб'єктів даних. У цьому контексті це означає, що під час обробки запиту мають бути передбачені відповідні способи пошуку та отримання інформації про суб'єкта даних. Однак слід зазначити, що надмірне тлумачення в цьому відношенні може призвести до функцій пошуку та отримання інформації, які самі по собі становлять ризик для приватності суб'єктів даних. Тому важливо пам'ятати, що процес пошуку даних також повинен бути розроблений у дружній до захисту даних спосіб, щоб він не ставив під загрозу приватність інших осіб, наприклад, працівників контролера.

5.2 Належні заходи для надання доступу

5.2.1 Вжиття «відповідних заходів»

127. Стаття 12 GDPR встановлює вимоги до надання доступу, тобто до надання підтвердження, персональних даних та додаткової інформації відповідно до статті 15, а також визначає форму, спосіб і терміни надання права на доступ. «Настанови щодо прозорості відповідно до Регламенту 2016/679» Робочої групи за статтею 29[76] надає подальші вказівки щодо статті 12, переважно стосовно статей 13 та 14 GDPR, а також щодо статті 15 та прозорості в цілому. Таким чином, те, що визначено в цих настановах, часто може однаково застосовуватися щодо надання доступу відповідно до статті 15.

128. Стаття 12(1) GDPR зазначає, що контролер повинен вжити належних заходів для надання будь-якого повідомлення відповідно до статті 15, що стосується обробки, суб'єкту даних у стислій, прозорій, зрозумілій та доступній формі, використовуючи чітку та просту мову. Стаття 12(2) передбачає, що контролер повинен сприяти здійсненню суб'єктом даних права на доступ. Більш точні вимоги в цьому відношенні повинні оцінюватися в кожному конкретному випадку. Вирішуючи, які заходи є доцільними, контролери повинні враховувати всі відповідні обставини, включаючи, але не обмежуючись ними, обсяг даних, що обробляються, складність обробки даних та знання, якими вони володіють про своїх суб'єктів даних, наприклад, якщо більшість суб'єктів даних є дітьми, людьми похилого віку або особами з інвалідністю. Крім того, в ситуаціях, коли контролеру стає відомо про особливі потреби суб'єкта даних, який подає запит, наприклад, через додаткову інформацію в запиті, контролер повинен враховувати ці обставини. Як наслідок, відповідні заходи будуть відрізнятися.

129. При проведенні оцінки важливо пам'ятати, що термін «відповідний» ніколи не слід розуміти як спосіб обмеження обсягу даних, на які поширюється право на доступ. Термін «відповідний» не означає, що зусилля з надання інформації можуть бути збалансовані, наприклад, з будь-яким інтересом, який може мати суб'єкт даних в отриманні персональних даних. Натомість оцінка повинна бути спрямована на вибір найбільш відповідного методу надання всієї інформації, охопленої цим правом, залежно від конкретних обставин у кожному конкретному випадку. Як

[76] Настанови щодо прозорості відповідно до Регламенту 2016/679 – схвалені EDPB (далі — «Настанови Робочої групи за статтею 29 щодо прозорості – схвалені EDPB») Робочої групи за статтею 29, РД 260, версія 01, 11 квітня 2018 року.

наслідок, контролер, який обробляє велику кількість даних у великих масштабах, повинен докласти значних зусиль, щоб забезпечити право на доступ до даних для суб'єктів даних у стислій, прозорій, зрозумілій та доступній формі, використовуючи просту та чітку мову.

130. Необхідно уникати направлення суб'єкта даних до різних джерел у відповідь на запит про отримання доступу до даних. Як раніше зазначалося в Настановах Робочої групи за статтею 29 щодо прозорості (щодо поняття «надання» в статтях 13 і 14 GDPR), поняття «надання» означає, що *«суб'єкт даних не повинен активно шукати інформацію, охоплену цими статтями, серед іншої інформації, наприклад, умов використання вебсайту або додатка»*[77]. Таким чином, з огляду на принцип прозорості, суб'єкти даних повинні отримувати від контролера інформацію та персональні дані, які вимагаються статей 15(1), 15(2) та 15(3), у спосіб, що забезпечує повний доступ до запитуваної інформації. За особливих обставин обмін інформацією всередині контролера може бути недоцільним або навіть незаконним, наприклад, через конфіденційний характер інформації (наприклад, інформація, що стосується викривання). У таких випадках буде доцільно розділити інформацію на кілька відповідей у відповідь на запит суб'єкта даних про надання доступу до неї. Метод, обраний контролером, повинен фактично надавати суб'єкту даних запитувані дані та інформацію, отже, було б недоцільно лише пропонувати суб'єкту даних перевірити запитувані дані, що зберігаються на його власному пристрої, зокрема перевірити історію кліків та IP-адреси на його мобільному телефоні.

131. Відповідно до принципу підзвітності, контролер повинен задокументувати свій підхід, щоб мати можливість довести, наскільки засоби, обрані для надання необхідної інформації відповідно до статті 5, відповідають обставинам, що склалися.

5.2.2 Різні способи надання доступу

132. Як вже пояснювалося в розділі 2.2.2 вище, подаючи запит на отримання доступу, суб'єкти даних мають право отримати копію своїх даних, які обробляються відповідно до статті 15(3), разом із додатковою інформацією, що вважається основним способом надання доступу до персональних даних.

133. Однак за певних обставин для контролера може бути доцільним надати доступ в інший спосіб, ніж надання копії. Такими непостійними способами надання доступу до даних можуть бути, зокрема, усна інформація, перевірка файлів, доступ на місці або віддалений доступ без можливості завантаження. Ці способи можуть бути прийнятними для надання доступу, наприклад, у випадках, коли відповідає інтересам суб'єкта даних або коли суб'єкт даних просить про це. Доступ на місці також може бути доцільним, як початковий захід, коли контролер обробляє велику кількість нецифрових даних, щоб дозволити суб'єкту даних бути поінформованим про те, які персональні дані обробляються, і мати можливість прийняти обґрунтоване рішення про те, які персональні дані він або вона хоче отримати в копії. Непостійні способи надання доступу можуть бути достатніми та відповідними в певних ситуаціях; наприклад, вони можуть задовольнити потребу суб'єктів даних у перевірці правильності даних, які обробляються контролером, шляхом надання суб'єктам даних можливості переглянути

[77] Настанови Робочої групи за статтею 29 щодо прозорості – схвалені EDPB, пункт 33.

оригінальні дані. Контролер не зобов'язаний надавати інформацію в інший спосіб, окрім надання копії, але повинен застосовувати обґрунтований підхід при розгляді такого запиту. Надання доступу в інший спосіб, ніж надання копії, не позбавляє суб'єктів даних права на отримання копії, якщо тільки вони не вирішили цього не робити.

134. Контролер може вирішити, залежно від конкретної ситуації, надати копію даних, що обробляються, разом із додатковою інформацією, у різний спосіб, наприклад, електронною поштою, звичайною поштою або за допомогою інструмента самообслуговування. Якщо суб'єкт даних подає запит електронними засобами, і якщо суб'єкт даних не вимагає іншого, інформація повинна бути надана в загальноприйнятій електронній формі, як зазначено в статті 15(3). У будь-якому випадку, контролер повинен розглянути відповідні технічні та організаційні заходи, включаючи належне шифрування, при наданні інформації електронною поштою або за допомогою онлайн-інструментів самообслуговування.

135. У ситуації, коли контролер обробляє персональні дані про особу, яка подає запит, у невеликому обсязі, копія персональних даних та додаткова інформація можуть і повинні бути надані за допомогою простої процедури.

> **Приклад 22:** Місцевий книжковий магазин веде облік імен та адрес своїх клієнтів, які замовили доставку додому. Покупець відвідує книжковий магазин і подає запит на отримання доступу до даних. У цій ситуації було б достатньо роздрукувати персональні дані клієнта безпосередньо з бізнес-системи, надавши при цьому додаткову інформацію, передбачену статтями 15(1) і (2).

> **Приклад 23:** Щомісячний донор благодійної організації надсилає запит на отримання доступу електронною поштою. Благодійна організація зберігає інформацію про пожертви, зроблені за останні дванадцять місяців, а також імена та електронні адреси донорів. Контролер може надати копію персональних даних та додаткову інформацію, відповівши на електронний лист, за умови застосування всіх необхідних запобіжних заходів, беручи до уваги, наприклад, характер даних.

136. Навіть контролери, які обробляють велику кількість даних, можуть вирішити покладатися на ручні процедури для обробки запитів на отримання доступу. Якщо контролер обробляє дані в декількох різних підрозділах, йому необхідно зібрати персональні дані з кожного підрозділу, щоб мати можливість відповісти на запит суб'єкта даних.

> **Приклад 24:** Адміністратор призначається контролером для вирішення практичних питань, пов'язаних із запитами на отримання доступу. Отримавши запит, адміністратор надсилає запит електронною поштою до різних відділів організації з проханням зібрати персональні дані про суб'єкта даних. Представники кожного відділу надають адміністратору персональні дані, які обробляє їхній відділ. Потім адміністратор надсилає всі персональні дані суб'єкту даних разом із необхідною додатковою інформацією, наприклад, електронною поштою.

137. Хоча ручні процеси обробки запитів на отримання доступу можуть розглядатися як належні, деякі контролери можуть отримати вигоду від використання автоматизованих процесів для обробки запитів суб'єктів даних. Це може бути, зокрема, у випадку контролерів, які отримують велику кількість запитів. Одним зі способів надання інформації, передбаченої статтею 15, є

надання суб'єкту даних інструментів самообслуговування. Це може сприяти ефективній та своєчасній обробці запитів суб'єктів даних на отримання доступу, а також дозволить контролеру включити механізм перевірки в інструмент самообслуговування.

Приклад 25: Соціальна мережа має автоматизований процес обробки запитів на отримання доступу, який дозволяє суб'єкту даних отримати доступ до своїх персональних даних зі свого облікового запису користувача. Щоб отримати персональні дані, користувачі соціальних мереж можуть вибрати опцію «Завантажити свої персональні дані» при вході до свого облікового запису. Ця опція самообслуговування дозволяє користувачам завантажити файл, що містить їхні персональні дані, безпосередньо з облікового запису користувача на власний комп'ютер.

138. Використання інструментів самообслуговування ніколи не повинно обмежувати обсяг отриманих персональних даних. Якщо неможливо надати всю інформацію, передбачену статтею 15, за допомогою інструмента самообслуговування, решту інформації необхідно надати в інший спосіб. Контролер дійсно може заохочувати суб'єкта даних використовувати інструмент самообслуговування, який він створив для обробки запитів на отримання доступу. Однак слід зазначити, що контролер також повинен обробляти запити на отримання доступу, які не надсилаються через встановлений канал зв'язку[78].

5.2.3 Надання доступу в «стислій, прозорій, зрозумілій та доступній формі з використанням чіткої та простої мови»

139. Відповідно до статті 12(1) GDPR, контролер повинен вжити належних заходів для забезпечення доступу згідно зі статтею 15 у стислій, прозорій, зрозумілій та доступній формі, використовуючи чітку та просту мову.

140. Вимога щодо надання доступу суб'єкту даних у стислій та прозорій формі означає, що контролери повинні представляти інформацію ефективно та лаконічно, щоб вона була легко зрозумілою суб'єкту даних, особливо якщо це дитина. Контролер повинен враховувати кількість і складність даних при виборі способу надання доступу відповідно до статті 15.

Приклад 26: Провайдер соціальних мереж обробляє велику кількість інформації про суб'єкта даних. Значна частина цих персональних даних — це інформація, що міститься на сотнях сторінок лог-файлів, де реєструються дії суб'єкта даних на вебсайті. Якщо суб'єкти даних вимагають надання доступу до своїх персональних даних, то на персональні дані в цих лог-файлах дійсно поширюється право на доступ. Таким чином, право на доступ може бути формально реалізоване, якщо суб'єкту даних будуть надані ці сотні сторінок лог-файлів. Однак, якщо не вжити заходів для полегшення розуміння інформації, що міститься в лог-файлах, право суб'єкта даних на доступ може не бути реалізоване на практиці, оскільки з лог-файлів неможливо легко отримати будь-яку інформацію, а отже, не виконати вимогу статті 12(1) GDPR. Тому контролер повинен бути обережним і ретельним при виборі способу представлення інформації та персональних даних суб'єкту даних.

[78] Див. розділ 3.1.2.

141. За обставин, зазначених у наведеному вище прикладі, використання багаторівневого підходу, подібного до багаторівневого підходу, запропонованого в Настановах щодо прозорості повідомлень про конфіденційність[79], може бути відповідним заходом для виконання вимог статей 15 та 12(1) GDPR. Це питання буде більш детально розглянуто в розділі 5.2.4. нижче. Вимога, щоб інформація була «зрозумілою», означає, що вона повинна бути зрозумілою цільовій аудиторії[80], враховуючи при цьому будь-які особливі потреби суб'єкта даних, які можуть бути відомі контролеру[81]. Оскільки право на доступ часто дозволяє здійснювати інші права суб'єкта даних, дуже важливо, щоб надана інформація була зрозумілою та чіткою. Це пов'язано з тим, що суб'єкти даних зможуть розглянути питання про те, чи скористатися своїм правом, наприклад, на виправлення відповідно до статті 16 GDPR, лише після того, як вони знатимуть, які персональні дані обробляються, з якою метою тощо. Як наслідок, контролеру може знадобитися надати суб'єкту даних додаткову інформацію, яка пояснює надані дані. Слід підкреслити, що складність обробки даних зобов'язує контролера забезпечити засоби для того, щоб зробити дані зрозумілими, і не може бути використаний як аргумент для обмеження доступу до всіх даних. Аналогічно, обов'язок контролера надавати дані у стислій формі не може бути використаний як аргумент для обмеження доступу до всіх даних.

Приклад 27: Вебсайт електронної комерції збирає дані про товари, переглянуті або придбані на його вебсайті, для маркетингових цілей. Частина цих даних буде складатися з даних у необробленому форматі[82], які не були проаналізовані й можуть не мати прямого значення для читача (коди, історія активності тощо). Такі дані, пов'язані з діяльністю суб'єктів даних, також підпадають під дію права на доступ і, як наслідок, повинні бути надані суб'єкту даних у відповідь на запит про отримання доступу. При наданні даних у необробленому форматі важливо, щоб контролер вжив необхідних заходів для забезпечення розуміння даних суб'єктом даних, наприклад, надавши пояснювальний документ, який переводить необроблений формат у зручну для користувача форму. Крім того, такий документ може пояснити, що скорочення та інші акроніми, наприклад, «А» означає, що покупку було перервано, а «В» означає, що покупку було здійснено.

142. Аспект «доступність» означає, що інформація, передбачена в статті 15, повинна бути представлена у спосіб, який полегшує доступ до неї суб'єкту даних. Це стосується, зокрема, макета, відповідних заголовків та абзаців. Інформація завжди повинна надаватися простою та зрозумілою мовою. Контролер, який пропонує послугу в країні, повинен також надавати відповіді мовою, зрозумілою суб'єктам даних у цій країні. Також заохочується використання

---

[79] Настанови Робочої групи за статтею 29 щодо прозорості – схвалені EDPB, пункт 35.

[80] Зрозумілість тісно пов'язана з вимогою використовувати просту та зрозумілу мову (Настанови щодо прозорості Робочої групи за статтею 29, схвалені EDPB, п. 9). Те, що сказано про просту та зрозумілу мову в п. 12-16 щодо інформації, про яку йдеться в статтях 13 і 14 GDPR, однаково стосується і повідомлень, передбачених статтею 15.

[81] Див. п. 128.

[82] Під сирим форматом у прикладі слід розуміти неаналізовані дані, що лежать в основі обробки, а не найнижчий рівень сирих даних, які можуть бути лише машинозчитуваними (наприклад, «біти»).

стандартних іконок, якщо це полегшує зрозумілість і доступність інформації. Якщо запит на отримання інформації стосується суб'єктів даних із вадами зору або інших суб'єктів даних, які можуть мати труднощі з доступом до інформації або її розумінням, очікується, що контролер вживатиме заходів, що полегшують розуміння наданої інформації, включаючи усну інформацію, коли це є обґрунтованим[83]. Контролер повинен приділяти особливу увагу тому, щоб люди похилого віку, діти, особи з вадами зору або особи з когнітивними чи іншими обмеженими можливостями могли реалізовувати свої права, наприклад, заздалегідь надаючи доступні аспекти, що полегшують реалізацію цих прав.

5.2.4 Велика кількість інформації зумовлює особливі вимоги до способу її надання

143. Незалежно від засобів, що використовуються для надання доступу, може виникнути суперечність між обсягом інформації, яку контролер повинен надати суб'єктам даних, та вимогою, що вона має бути стислою. Одним зі способів досягнення обох цілей, а також прикладом відповідного заходу для деяких контролерів, коли необхідно надати велику кількість даних, є використання багаторівневого підходу. Такий підхід може полегшити розуміння даних суб'єктами даних. Однак слід підкреслити, що цей підхід може бути використаний лише за певних обставин і повинен здійснюватися таким чином, щоб не обмежувати право на доступ, як пояснюється нижче. Крім того, використання багаторівневого підходу не повинно створювати додатковий тягар для суб'єкта даних. Отже, він найкраще підходить, коли доступ надається в онлайновому контексті. Багаторівневий підхід — це лише спосіб представити інформацію, передбачену в статті 15, у спосіб, який також відповідає вимогам статті 12(1) GDPR, і його не слід плутати з можливістю контролерів вимагати від суб'єкта даних вказати інформацію або діяльність з обробки, до якої відноситься запит, як це передбачено в преамбулі 63 GDPR[84].

144. Багаторівневий підхід до права на доступ означає, що контролер, за певних обставин, може надавати персональні дані та додаткову інформацію, що вимагається відповідно до статті 15, на різних рівнях. Перший рівень повинен включати інформацію про обробку та права суб'єкта даних відповідно до статей 15(1)(a)-(h) та 15(2), а також першу частину оброблених персональних даних. На другому рівні слід надати більше персональних даних.

145. Вирішуючи, яку інформацію слід надавати на різних рівнях, контролер повинен враховувати, яку інформацію суб'єкт даних загалом вважав би найбільш релевантною. Відповідно до принципу справедливості, перший рівень також повинен містити інформацію про обробку, яка має найбільший вплив на суб'єкта даних[85]. Контролери повинні довести підзвітність щодо своїх міркувань, викладених вище.

---

[83] Див. Настанови Робочої групи за статтею 29 щодо прозорості – схвалені EDPB, пункт 21.

[84] Див. також розділ 2.3.1.

[85] Див. Настанови Робочої групи за статтею 29 щодо прозорості – схвалені EDPB, пункт 36.

Приклад 28: Контролер аналізує великі масиви даних, щоб розподілити клієнтів на різні сегменти залежно від їхньої поведінки в Інтернеті. У цій ситуації можна припустити, що найбільш важливою для суб'єктів даних є інформація про те, до якого сегменту їх було віднесено. Як наслідок, ця інформація повинна бути включена до першого рівня. Дані в необробленому форматі[86], які ще не були проаналізовані або додатково оброблені, такі як активність користувачів на вебсайті, також є персональними даними, на які поширюється право на доступ, проте в деяких випадках може бути достатньо надати цю інформацію на іншому рівні.

146. Для того, щоб використання багаторівневого підходу вважалося належним заходом, необхідно, щоб суб'єкт даних був із самого початку поінформований про те, що інформація, передбачена в статті 15, структурована на різні рівні, а також надано опис того, які персональні дані та інформація будуть міститися на різних рівнях. Таким чином, суб'єкту даних буде легше вирішити, до яких рівнів він хоче отримати доступ. Опис повинен об'єктивно відображати всі категорії персональних даних, які фактично обробляються контролером. Також має бути зрозуміло, як суб'єкт даних може отримати доступ до різних рівнів. Доступ до різних рівнів не повинен вимагати від суб'єкта даних необґрунтованих зусиль і не повинен бути обумовлений формулюванням нового запиту суб'єкта даних. Це означає, що суб'єкти даних повинні мати можливість вибирати, чи отримувати доступ до всіх рівнів одночасно, чи до одного або двох рівнів, якщо їх це влаштовує.

Приклад 29: Суб'єкт даних робить запит на отримання доступу до сервісу потокового відео. Запит робиться через опцію, яка доступна, коли суб'єкт даних увійшов у свій обліковий запис. Суб'єкту даних пропонується два варіанти, які відображаються у вигляді кнопок на вебсторінці. Перший варіант — завантажити 1 частину персональних даних та додаткову інформацію. Вона містить, зокрема, нещодавню історію потокового мовлення, інформацію про обліковий запис та платіжну інформацію. Другий варіант — завантажити 2 частину персональних даних, яка містить технічні файли журналів про діяльність суб'єкта даних та історичну інформацію про обліковий запис. У цьому випадку контролер надав можливість суб'єктам даних реалізувати своє право таким чином, щоб не створювати додатковий тягар для суб'єкта даних.

Варіант 1: У випадках, коли суб'єкт даних вибирає тільки кнопку для завантаження 1 частини персональних даних, контролер зобов'язаний надати тільки 1 частину даних.

Варіант 2: У випадках, коли суб'єкт даних вибирає кнопки як для 1 частини, так і для 2 частини даних, контролер не може передавати тільки 1 частину даних і просити нового підтвердження перед передачею 2 частини даних. Натомість суб'єкту даних повинні бути надані обидві частини даних, як це випливає з поданого запиту.

147. Використання багаторівневого підходу не вважається доцільним для всіх контролерів або в усіх ситуаціях. Його слід застосовувати лише тоді, коли суб'єкту даних буде важко зрозуміти інформацію, якщо вона буде надана в повному обсязі. Іншими словами, контролер повинен

[86] Див. виноску 82.

довести, що використання багаторівневого підходу додає цінності для суб'єкта даних, допомагаючи йому зрозуміти надану інформацію. Таким чином, багаторівневий підхід вважатиметься доцільним лише тоді, коли контролер обробляє велику кількість персональних даних про суб'єкта даних, який подає запит, і коли суб'єкту даних буде очевидно складно зрозуміти або осмислити інформацію, якщо вона буде надана одразу. Той факт, що надання інформації, передбаченої статтею 15, сам по собі не є аргументом на користь використання багаторівневого підходу.

5.2.5 Формат

148. Відповідно до статті 12(1) GDPR, інформація, передбачена статтею 15, повинна надаватися в письмовій формі або іншими засобами, включаючи, за необхідності, електронні засоби. Що стосується доступу до персональних даних, які обробляються, то стаття 15(3) зазначає, що якщо суб'єкт даних подає запит електронними засобами, і якщо суб'єкт даних не вимагає іншого, інформація має бути надана в загальноприйнятій електронній формі. GDPR не визначає, що таке загальноприйнята електронна форма. Таким чином, існує кілька можливих форматів, які можна використовувати. Те, що вважається загальновживаною електронною формою, також змінюється з часом.

149. Визначення того, що можна вважати загальновживаною електронною формою, має ґрунтуватися на об'єктивній оцінці, а не на тому, який формат використовує контролер у своїй повсякденній діяльності. Для того, щоб визначити, який формат слід вважати загальновживаним у ситуації, що розглядається, контролер повинен оцінити, чи існують конкретні формати, які зазвичай використовуються у сфері діяльності контролера або в цьому контексті. Якщо таких форматів не існує, відкриті формати, встановлені міжнародними стандартами, такими як ISO, повинні, як правило, вважатися загальновживаними електронними форматами. Однак, EDPB не виключає можливості того, що інші формати також можуть вважатися загальновживаними в розумінні статті 15(3). При оцінці того, чи є формат загальновживаним електронним форматом, EDPB вважає, що важливим є те, наскільки легко особа може отримати доступ до інформації, наданої в поточному форматі. У зв'язку із цим слід зазначити, яку інформацію контролер надав суб'єкту даних про те, як отримати доступ до файлу, наданого в певному форматі, наприклад, які програми або програмне забезпечення можуть бути використані, щоб зробити формат більш доступним для суб'єкта даних. Однак суб'єкт даних не повинен бути зобов'язаний купувати програмне забезпечення, щоб отримати доступ до інформації.

150. Приймаючи рішення щодо формату, в якому має бути надана копія персональних даних та інформація, передбачена статтею 15, контролер повинен мати на увазі, що формат повинен дозволяти представляти інформацію в зрозумілій та доступній формі. Важливо, щоб суб'єкту даних надавалася інформація в закріпленому, постійному вигляді (текстовому, електронному). Оскільки інформація повинна зберігатися протягом тривалого часу, інформація в письмовій формі, в тому числі за допомогою електронних засобів, у цілому, є кращою за інші форми. Копія персональних даних може, за необхідності, зберігатися на електронному носії, такому як компакт-диск або USB.

151. Слід зазначити, що для того, щоб контролер міг вважати, що суб'єктам даних було надано копію персональних даних, недостатньо надати їм доступ до їхніх персональних даних. Для того, щоб вимога про надання копії персональних даних була виконана, і якщо дані надаються в

електронному/цифровому вигляді, суб'єкти даних повинні мати можливість завантажити свої дані в загальноприйнятій електронній формі.

152. Відповідальність за прийняття рішення про відповідну форму, в якій будуть надаватися персональні дані, лежить на контролері. Контролер може, хоча і не обов'язково зобов'язаний, надавати документи, які містять персональні дані про суб'єктів даних, що подають запит, в їх оригінальній формі. Контролер може, зокрема, у кожному конкретному випадку надавати доступ до копії носія як такого, враховуючи необхідність забезпечення прозорості (наприклад, для перевірки точності даних, якими володіє контролер, у разі запиту на отримання доступу до медичної картки або аудіозапису, розшифрування якого оскаржується). Однак Суд ЄС у своєму тлумаченні права на доступ відповідно до Директиви 95/46/ЄС зазначив, що «для дотримання *[права на доступ]* достатньо, щоб заявнику було надано повне резюме цих даних у зрозумілій формі, тобто у формі, яка дозволяє йому ознайомитися із цими даними та перевірити, чи є вони точними та обробляються відповідно до цієї директиви, щоб він міг, у відповідних випадках, скористатися наданими йому правами» [87]. На відміну від директиви, GDPR прямо містить зобов'язання надавати суб'єкту даних копію персональних даних, які обробляються. Проте це не означає, що суб'єкт даних завжди має право отримати копію документів, що містять персональні дані, а лише незмінену копію персональних даних, які обробляються в цих документах. [88]Така копія персональних даних може бути надана у вигляді зведення, що містить усі персональні дані, на які поширюється право на доступ, якщо таке зведення дозволяє суб'єкту даних бути поінформованим та перевірити законність обробки. Таким чином, між формулюванням GDPR та рішенням Суду ЄС із цього питання немає жодних суперечностей. Слово «резюме» в рішенні не слід тлумачити як таке, що означає, що компіляція не охоплюватиме всі дані, на які поширюється право на доступ, а є лише способом представлення всіх цих даних без надання доступу до первинних документів, які містять персональні дані. Оскільки компіляція повинна містити копію персональних даних, слід підкреслити, що вона не може бути зроблена у спосіб, який будь-яким чином змінює або доповнює зміст інформації.

[87] Суд ЄС, об'єднані справи C-141/12 та 372/12, YS та інші, п. 60.

[88] Питання, пов'язані із цією темою, є предметом розгляду у справах, які наразі перебувають на розгляді в Суді ЄС (C-579/21 та C-307/21).

Прийнято

Приклад 30: Суб'єкт даних був застрахований у страховій компанії протягом багатьох років. Сталося кілька страхових випадків. У кожному випадку між суб'єктом даних і страховою компанією велася письмова переписка електронною поштою. Оскільки суб'єкт даних повинен був надати інформацію про конкретні обставини кожного інциденту, листування містить багато особистої інформації про суб'єкта даних (хобі, сусіди по квартирі, щоденні звички і т.д.). У деяких випадках виникали розбіжності щодо зобов'язання страхової компанії виплатити компенсацію суб'єкту даних, що призводило до значної кількості листування туди і назад. Усе це листування зберігається в страховій компанії. Суб'єкт даних подає запит на отримання доступу. У цій ситуації контролер не обов'язково повинен надавати електронні листи в оригінальній формі, пересилаючи їх суб'єкту даних. Замість цього контролер може скомпілювати електронну кореспонденцію, що містить персональні дані суб'єкта даних, у файл, який надається суб'єкту даних.

153. Незалежно від форми, в якій контролер надає персональні дані, наприклад, шляхом надання фактичних документів, що містять персональні дані, або компіляції персональних даних, інформація повинна відповідати вимогам прозорості, викладеним у статті 12 GDPR. У деяких випадках способом дотримання цих вимог може бути створення певної компіляції та/або вилучення даних у спосіб, який робить інформацію легкою для сприйняття, що може бути способом дотримання цих вимог. В інших випадках інформацію краще зрозуміти, надавши копію документа, що містить персональні дані. Таким чином, рішення про те, яка форма є найбільш підходящою, має прийматися в кожному конкретному випадку окремо.

154. У цьому контексті важливо пам'ятати, що існує різниця між правом на доступ, передбаченим статтею 15 GDPR, та правом на отримання копії адміністративних документів, яке регулюється національним законодавством, причому останнє є правом на отримання копії самого документа. Це не означає, що право на доступ, передбачене статтею 15 GDPR, виключає можливість отримати копію документа/носія, на якому містяться персональні дані.

155. У деяких випадках самі персональні дані встановлюють вимоги до того, в якому форматі вони повинні бути надані. Наприклад, якщо персональні дані є рукописною інформацією суб'єкта даних, суб'єкту даних може знадобитися надати фотокопію цієї рукописної інформації, оскільки сам почерк являє собою персональні дані. Особливо це стосується випадків, коли почерк є важливим для обробки, наприклад, для аналізу рукописних текстів. Те ж саме стосується й аудіозаписів, оскільки голос суб'єкта даних сам по собі є персональними даними. Однак у деяких випадках доступ може бути наданий шляхом надання транскрипції розмови, наприклад, якщо це погоджено між суб'єктом даних і контролером.

156. Слід зазначити, що положення про вимоги до формату відрізняються щодо права на доступ та права на перенесення даних. У той час як право на перенесення даних відповідно до статті 20 GDPR вимагає, щоб інформація була надана в машинозчитуваному форматі, право на інформацію за статтею 15 цього не вимагає. Таким чином, формати, які вважаються неприйнятними для виконання запиту на перенесення даних, наприклад, pdf-файли, можуть бути прийнятними для виконання запиту на отримання доступу до інформації.

5.3 Терміни надання доступу

157. Стаття 12(3) GDPR вимагає, щоб контролер надавав суб'єкту даних інформацію про дії, вжиті щодо запиту відповідно до статті 15, без невиправданої затримки та в будь-якому випадку протягом одного місяця з моменту отримання запиту. Цей термін може бути продовжений максимум на два місяці з урахуванням складності та кількості запитів, за умови, що суб'єкт даних був поінформований про причини такої затримки протягом одного місяця з моменту отримання запиту. Це зобов'язання інформувати суб'єкта даних про продовження терміну та його причини не слід плутати з інформацією, яка повинна бути надана невідкладно та не пізніше одного місяця, коли контролер не вживає заходів за запитом, як це детально описано в статті 12(4) GDPR.

158. Контролер повинен реагувати та, як правило, надавати інформацію, передбачену статтею 15, без невиправданої затримки, що означає, що інформація повинна бути надана якомога швидше. Це означає, що якщо є можливість надати запитувану інформацію в коротший термін, ніж один місяць, контролер повинен це зробити. EDPB також вважає, що терміни надання відповіді на запит у деяких ситуаціях повинні бути адаптовані до періоду зберігання інформації, щоб мати можливість забезпечити доступ до неї[89].

159. Відлік терміну починається з моменту отримання контролером запиту за статтею 15, тобто коли запит потрапляє до контролера через один з його офіційних каналів.[90] Не обов'язково, щоб контролер знав про запит. Однак, якщо контролеру необхідно зв'язатися із суб'єктом даних через невизначеність щодо особи, яка подала запит, може відбутися призупинення в часі до отримання контролером необхідної інформації від суб'єкта даних, за умови, що контролер запросив додаткову інформацію без невиправданої затримки. Те саме стосується випадків, коли контролер просить суб'єкта даних вказати операції з обробки, яких стосується запит, якщо дотримані умови, викладені в преамбулі 63[91].

> **Приклад 31**: Після отримання запиту контролер негайно реагує і запитує інформацію, необхідну для підтвердження особи, яка подала запит. Особа відповідає лише через кілька днів, а інформація, яку суб'єкт даних надсилає для підтвердження особи, здається недостатньою, що змушує контролера звернутися за роз'ясненнями. У такій ситуації відбувається призупинення в часі, поки контролер не отримає достатньо інформації для підтвердження особи суб'єкта даних.

160. Період часу для відповіді на запит про отримання доступу повинен розраховуватися відповідно до Регламенту № 1182/71[92].

---

[89] Див. розділ 2.3.3

[90] У деяких країнах-членах ЄС існує національне законодавство, яке визначає, коли повідомлення вважається отриманим, з урахуванням вихідних та національних свят.

[91] Див. далі розділ 2.3.1.

[92] Регламент Ради (ЄЕП, ЄВРОАТОМ) № 1182/71 від 3 червня 1971 року, що визначає правила, які застосовуються до періодів, дат і термінів.

Приклад 32: Організація отримує запит 5 березня. Відлік часу починається з того ж дня. Це дає організації час до 5 квітня включно, щоб задовольнити запит, найпізніше — до 5 квітня.

Приклад 33: Якщо організація отримує запит 31 серпня, а оскільки наступний місяць коротший і відповідної дати немає, то датою надання відповіді буде найпізніше останній день наступного місяця, тобто 30 вересня.

161. Якщо останній день цього періоду припадає на вихідний або святковий день, контролер має надати відповідь до наступного робочого дня.

162. За певних обставин контролер може продовжити час для відповіді на запит про отримання доступу до інформації ще на два місяці, якщо це необхідно, беручи до уваги складність та кількість запитів. Слід підкреслити, що ця можливість є винятком із загального правила і нею не слід зловживати. Якщо контролери часто змушені продовжувати терміни, це може свідчити про необхідність подальшого розвитку загальних процедур обробки запитів.

163. Те, що є складним запитом, залежить від конкретних обставин кожної справи. Деякі з факторів, які можна вважати релевантними, є, зокрема, такими:

- обсяг даних, які обробляє контролер;
- спосіб зберігання інформації, особливо якщо її важко отримати, наприклад, коли дані обробляються різними підрозділами організації;
- необхідність редагування інформації, коли застосовується виняток, наприклад, інформації, що стосується інших суб'єктів даних або становить комерційну таємницю, а також
- коли інформація потребує подальшої обробки для того, щоб бути зрозумілою.

164. Той факт, що виконання запиту вимагатиме значних зусиль, не робить запит складним. Аналогічно, той факт, що велика компанія отримує велику кількість запитів, не призведе до автоматичного продовження терміну. Однак, коли контролер тимчасово отримує велику кількість запитів, зокрема у зв'язку з надзвичайним розголосом його діяльності, це може розглядатися як законна причина для подовження термінів надання відповіді. Проте контролер, особливо той, який обробляє велику кількість даних, повинен мати процедури та механізми, які дозволять йому обробляти запити у встановлені терміни за звичайних обставин.

6 ЛІМІТИ ТА ОБМЕЖЕННЯ ПРАВА НА ДОСТУП

6.1 Загальні зауваження

165. Право на доступ підлягає обмеженням, які випливають зі статті 15(4) GDPR (права інших осіб) та статті 12(5) GDPR (явно необґрунтовані або надмірні запити). Крім того, законодавство Союзу або держав-членів може обмежувати право на доступ відповідно до статті 23 GDPR. Винятки щодо обробки персональних даних для наукових, історичних досліджень, статистичних цілей або цілей архівування в суспільних інтересах можуть ґрунтуватися на статтях 89(2) та 89(3) GDPR, відповідно, а відступи щодо обробки, яка здійснюється в журналістських цілях або з метою

академічного, художнього чи літературного вираження, можуть ґрунтуватися на статті 85(2) GDPR.

166. Важливо зазначити, що, окрім вищезазначених лімітів, відступів та можливих обмежень, GDPR не допускає жодних інших винятків або відступів від права на доступ. Це означає, *серед іншого*, що право на доступ не містить жодних загальних застережень щодо обґрунтованості зусиль, які повинен докласти контролер, щоб задовольнити запит суб'єкта даних відповідно до статті 15 GDPR[93]. Крім того, не дозволяється обмежувати або звужувати право на доступ у договорі між контролером і суб'єктом даних.

167. Відповідно до преамбули 63, право на доступ надається суб'єктам даних для того, щоб бути поінформованими та перевіряти законність обробки. Право на доступ дозволяє суб'єкту даних, *серед іншого*, отримати, залежно від обставин, виправлення, видалення або блокування персональних даних [94]. При цьому суб'єкти даних не зобов'язані вказувати причини або обґрунтовувати свій запит. До тих пір, поки вимоги статті 15 GDPR виконуються, цілі, що лежать в основі запиту, повинні розглядатися як нерелевантні[95].

6.2 Стаття 15(4) GDPR

168. Відповідно до статті 15(4) GDPR право на отримання копії не повинно негативно впливати на права й свободи інших осіб. Пояснення щодо цього обмеження наведено в п'ятому та шостому реченнях преамбули 63. Це право не повинно негативно впливати на права та свободи інших осіб, у тому числі на комерційну таємницю або інтелектуальну власність, зокрема на авторське право, що захищає програмне забезпечення. Однак результатом цих міркувань не повинна бути відмова у наданні всієї інформації суб'єкту даних. При тлумаченні статті 15(4) GDPR слід проявляти особливу обережність, щоб не допустити невиправданого розширення обмежень, викладених у статті 23 GDPR, які допустимі лише за суворих умов.

169. Стаття 15(4) GDPR застосовується до права на отримання копії даних, що є основним способом надання доступу до оброблених даних (другий компонент права на доступ). Він також застосовується, і права та свободи інших осіб повинні бути враховані, якщо доступ до персональних даних у виняткових випадках надається в інший спосіб, ніж копія. Наприклад, немає ніякої різниці, чи зачіпає комерційну таємницю надання копії або надання доступу на місці суб'єкту даних Стаття 15(4) GDPR не застосовується до додаткової інформації про обробку, як зазначено в статті 15(1), підпункти a)-h) GDPR.

170. Згідно з преамбулою 63, суперечливі права та свободи включають комерційну таємницю або інтелектуальну власність і, зокрема, авторське право, що захищає програмне забезпечення. Ці

---

[93] Якщо контролер обробляє велику кількість інформації про суб'єкта даних, як зазначено в преамбулі 63 GDPR, контролер може попросити суб'єкта даних вказати інформацію або діяльність з обробки, якої стосується запит. Див. також розділ 2.3.1.

[94] Суд ЄС, об'єднані справи C-141/12 та C-372/12, YS та інші.

[95] Це не обмежує будь-яке застосовне національне законодавство, яке відповідає вимогам статті 23 GDPR, див. главу 6.4.

прямо згадані права та свободи слід розглядати лише як приклади, оскільки загалом будь-яке право або свобода, що ґрунтується на праві Союзу або держави-члена, може розглядатися як таке, що підпадає під обмеження, передбачене статтею 15(4) GDPR[96]. Таким чином, право на захист персональних даних (стаття 8 Європейської хартії основоположних прав) також може розглядатися як порушене право з точки зору статті 15(4) GDPR. Що стосується права на отримання копії, то право на захист даних інших осіб є типовим випадком, коли необхідно оцінити обмеження. Крім того, слід враховувати право на конфіденційність кореспонденції, наприклад, щодо приватного листування електронною поштою в контексті працевлаштування[97]. Важливо зазначити, що не кожен інтерес становить «права та свободи» відповідно до статті 15(4) GDPR. Наприклад, економічні інтереси компанії не розкривати персональні дані не досягають порогу для застосування винятку, передбаченого статтею 15(4), якщо це не стосується комерційної таємниці, інтелектуальної власності або інших захищених прав.

171. Інші» означає будь-яку іншу фізичну або юридичну особу, крім суб'єкта даних, яка реалізує своє право на доступ. Таким чином, можна було б розглянути права та свободи контролера або оператора (наприклад, щодо збереження комерційної таємниці та інтелектуальної власності). Якби законодавець ЄС хотів виключити права та свободи контролерів або операторів, він би використав термін «третя сторона», який визначений у статті 4(10) GDPR.

172. Загальне занепокоєння тим, що виконання запиту на отримання доступу може вплинути на права та свободи інших осіб, не є достатнім для того, щоб покладатися на статтю 15(4) GDPR. Контролер повинен довести, що в конкретній ситуації права чи свободи інших осіб дійсно будуть порушені.

> **Приклад 34:** Особа, яка зараз є повнолітньою, в минулому протягом кількох років перебувала під опікою служби у справах неповнолітніх. Відповідні файли можуть містити конфіденційну інформацію про інших осіб (батьків, соціальних працівників, інших неповнолітніх). Однак запит на отримання інформації від суб'єкта даних, як правило, не може бути відхилений із цієї причини з посиланням на статтю 15(4) GDPR. Навпаки, права та свободи інших осіб повинні бути детально вивчені та доведені службою у справах неповнолітніх як контролером. Залежно від інтересів, про які йдеться, та їхньої відносної ваги, надання такої конкретної інформації може бути відхилено (наприклад, шляхом редагування імен).

173. Що стосується преамбули 4 GDPR та обґрунтування статті 52(1) Європейської хартії основоположних прав, право на захист персональних даних не є абсолютним правом[98]. Таким чином, здійснення права на доступ має бути збалансоване з іншими основоположними правами відповідно до принципу пропорційності. Якщо оцінка за статтею 15(4) GDPR доводить, що

---

[96] Вагомість або пріоритетність суперечливих прав і свобод не є питанням визначення термінів «права та свободи», однак, збалансування таких інтересів є частиною другого етапу оцінки, чи застосовується стаття 15(4). Див. п. 173 нижче.

[97] ЄСПЛ, справа «Bărbulescu проти Румунії», № 61496/08, п. 80, 5 вересня 2017 року.

[98] Див. для прикладу також Суд ЄС, об'єднані справи C-92/09 та C-93/09, Volker und Markus Schecke GbR та Hartmut Eifert проти землі Гессен [ВП], 9 листопада 2010 року, п. 48.

виконання запиту має несприятливі (негативні) наслідки для прав і свобод інших учасників (крок 1), необхідно зважити інтереси всіх учасників з урахуванням конкретних обставин справи та, зокрема, ймовірності та серйозності ризиків, пов'язаних із передачею даних. Контролер повинен спробувати узгодити суперечливі права (крок 2), наприклад, шляхом вжиття відповідних заходів, що зменшують ризик для прав і свобод інших осіб**.** Як підкреслено в преамбулі 63, захист прав і свобод інших осіб відповідно до статті 15(4) GDPR не повинен призводити до відмови в наданні всієї інформації суб'єкту даних. Це означає, що, якщо застосовується обмеження, інформацію, що стосується інших осіб, слід зробити нерозбірливою наскільки це можливо, замість того щоб відмовляти в наданні копії персональних даних. Однак, якщо неможливо знайти рішення щодо узгодження відповідних прав, контролер повинен на наступному етапі вирішити, які із суперечливих прав і свобод переважають (крок 3).

Приклад 35: Роздрібний торговець пропонує своїм клієнтам можливість замовляти товари через гарячу лінію, яку обслуговує його служба підтримки клієнтів. З метою доказу комерційних операцій підприємство роздрібної торгівлі зберігає запис дзвінків відповідно до суворих вимог чинного законодавства. Покупець хоче отримати копію розмови, яку він мав з агентом служби підтримки клієнтів. На першому етапі підприємство роздрібної торгівлі аналізує запит і розуміє, що запис містить персональні дані, які також стосуються іншої особи, а саме агента з обслуговування клієнтів. На другому етапі, щоб оцінити, чи вплине надання копії на права та свободи інших осіб, роздрібний торговець повинен збалансувати суперечливі інтереси, особливо беручи до уваги ймовірність і серйозність можливих ризиків для прав і свобод агента з обслуговування клієнтів, які присутні в повідомленні запису клієнту. Роздрібний торговець доходить висновку, що на записі міститься дуже обмежена кількість персональних даних, що стосуються агента з обслуговування клієнтів, лише його голос. Роздрібний торговець/контролер вважає, що агента нелегко ідентифікувати. Крім того, зміст дискусії мав професійний характер, а суб'єктом даних був співрозмовник. На підставі вищезазначених обставин контролер об'єктивно робить висновок, що право на доступ не впливає негативно на права та свободи агента з обслуговування клієнтів, а отже, контролер може надати суб'єкту даних повний запис, включаючи ті частини запису голосу, які стосуються агента з обслуговування клієнтів.

Приклад 36: Клієнтка магазину медичних товарів хоче отримати доступ до результатів вимірювань своїх ніг на підставі статті 15 GDPR. Магазин медичних товарів виміряв ноги суб'єкта даних, щоб виготовити індивідуальні компресійні панчохи. Очевидно, що магазин медичних товарів мав великий досвід і встановив спеціальну техніку для точного вимірювання. Після вимірювання в магазині клієнт хоче використати результати вимірювання, щоб купити дешевші шкарпетки в іншому місці (замовивши їх в інтернет-магазині). Магазин медичних товарів частково відмовляє в доступі до даних на підставі статті 15(4) GDPR, стверджуючи, що через особливі, точні методи вимірювання результати були захищені як комерційна таємниця. Якщо і тою мірою, у якій контролер зможе це довести:

- надання суб'єкту даних інформації про результати вимірювань неможливе без розкриття того, як були проведені вимірювання, та

- інформація про те, як були проведені вимірювання, включаючи, якщо це необхідно, точне визначення точок вимірювання, є комерційною таємницею,

він може застосувати статтю 15(4) GDPR.

Контролер все одно повинен буде надати якомога більше інформації про результати вимірювань, яка не розкриє його комерційну таємницю, навіть якщо це означатиме зусилля з перегляду та редагування результатів.

Приклад 37: ГРАВЕЦЬ X зареєстрований як користувач на ігровій платформі ПЛАТФОРМИ Y. Одного дня ГРАВЕЦЬ X отримує повідомлення про те, що доступ до його онлайн-акаунту обмежено. Оскільки він більше не може увійти в систему, ГРАВЕЦЬ X звертається до контролера з проханням надати доступ до всіх персональних даних, які його стосуються. Крім того, ГРАВЕЦЬ X вимагає доступ до причин обмеження акаунту. ПЛАТФОРМА Y, контролер ігрової онлайн-платформи, до якої було подано запит, інформує користувачів у своїх загальних положеннях та умовах, доступних на своєму вебсайті, що будь-який вид шахрайства (переважно за допомогою програмного забезпечення третіх осіб) призведе до тимчасової або постійної заборони доступу до її платформи. ПЛАТФОРМА Y також інформує користувачів у своїй політиці конфіденційності про обробку персональних даних з метою виявлення ігрового шахрайства, відповідно до вимог, викладених у статті 13 GDPR.

Після отримання запиту ГРАВЦЯ X про доступ, ПЛАТФОРМА Y повинна надати ГРАВЦЮ X копію персональних даних, які обробляються про ГРАВЦЯ X. Щодо причини обмеження доступу до акаунту, ПЛАТФОРМА Y повинна підтвердити ГРАВЦЮ X, що вона вирішила обмежити доступ ГРАВЦЯ X до онлайн-ігор у зв'язку з використанням одного або декількох ігрових видів шахрайства, які порушують загальні умови використання. На додаток до інформації, наданої про обробку з метою виявлення ігрового шахрайства, ПЛАТФОРМА Y повинна надати ГРАВЦЮ X доступ до інформації, яку вона зберігає про ігрові шахрайства ГРАВЦЯ X, що призвели до обмеження. Зокрема, ПЛАТФОРМА Y повинна надати ГРАВЦЮ X інформацію, яка призвела до обмеження доступу до акаунту (*наприклад*, огляд журналу, дату і час шахрайства, виявлення стороннього програмного забезпечення тощо), щоб суб'єкт даних (*тобто* ГРАВЕЦЬ X) міг переконатися в тому, що обробка даних була точною.

Однак, відповідно до статті 15(4) GDPR та преамбули 63 GDPR, ПЛАТФОРМА Y не зобов'язана розкривати будь-яку частину технічної роботи антишахрайського програмного забезпечення, навіть якщо ця інформація стосується ГРАВЦЯ X і може вважатися комерційною таємницею. Необхідний баланс інтересів відповідно до статті 15(4) GDPR призведе до того, що комерційна таємниця ПЛАТФОРМИ Y перешкоджатиме розкриттю цих персональних даних, оскільки знання технічної роботи антишахрайського програмного забезпечення може також дозволити користувачеві обійти майбутнє виявлення шахрайства або обману[99].

[99] Обсяг інформації, що надається фізичним особам, буде значною мірою залежати від контексту, враховуючи характер контролера та характер порушення умов надання послуг. У деяких випадках

174. Якщо контролери повністю або частково відмовляють у задоволенні запиту на отримання права на доступ відповідно до статті 15(4) GDPR, вони повинні негайно повідомити суб'єкта даних про причини, але не пізніше, ніж протягом одного місяця (стаття 12(4) GDPR). Пояснення повинно містити посилання на конкретні обставини, щоб суб'єкти даних могли оцінити, чи хочуть вони вживати заходів проти відмови. Воно повинна містити інформацію про можливість подання скарги до наглядового органу (стаття 77 GDPR) та звернення до суду (стаття 79 GDPR).

6.3 Стаття 12(5) GDPR

175. Стаття 12(5) GDPR дозволяє контролерам відхиляти запити на отримання права на доступ, які є явно необґрунтованими або надмірними. Ці поняття слід тлумачити обмежено, оскільки принципи прозорості та безоплатності прав суб'єктів даних не повинні бути підірвані.

176. Контролери повинні довести особі, чому вони вважають запит явно необґрунтованим або надмірним, і, якщо їх попросять, пояснити причини компетентному наглядовому органу. Кожен запит повинен розглядатися в кожному конкретному випадку в контексті, в якому він був зроблений, щоб вирішити, чи є він явно необґрунтованим або надмірним.

6.3.1 Що означає «явно необґрунтований»?

177. Запит на отримання права на доступ є явно необґрунтованим, якщо вимоги статті 15 GDPR явно та очевидно не виконуються при застосуванні об'єктивного підходу. Однак, як пояснювалося, зокрема, у розділі 3 вище, існує лише дуже мало передумов для запитів на отримання права на доступ. Тому EDPB підкреслює, що існує лише дуже обмежена можливість покладатися на «явно необґрунтовану» альтернативу статті 12(5) GDPR щодо запитів на отримання права на доступ.

178. Крім того, важливо нагадати, що перед тим, як застосувати обмеження, контролери повинні ретельно проаналізувати зміст та обсяг запиту. Наприклад, запит не слід вважати явно необґрунтованим, якщо він пов'язаний з обробкою персональних даних, на які не поширюється дія GDPR (у такому випадку запит взагалі не повинен розглядатися як запит за статтею 15).

179. Інші випадки, в яких застосування статті 12(5) GDPR є сумнівним, є запити, пов'язані з інформацією або діяльністю з обробки, які явно та очевидно не є предметом діяльності з обробки контролера.

> **Приклад 38**: Суб'єкт даних звертається із запитом до муніципального органу щодо даних, які обробляються державним органом. Замість того, щоб стверджувати, що запит є явно необґрунтованим, було б доцільніше і простіше для органу, до якого звертаються, підтвердити, що ці дані не обробляються цим органом (перший компонент статті 15 GDPR: «чи обробляються персональні дані»)[100].

контролер може надати лише основну інформацію у відповідь на запит про отримання доступу, до якого застосовується стаття 15(4).

[100] Інше питання полягає в тому, чи має право орган, якому адресовано запит на отримання доступу, передати запит до компетентного державного органу.

180. Контролер не повинен вважати запит явно необґрунтованим, якщо суб'єкт даних раніше подавав запити, які були явно необґрунтованими або надмірними, або якщо вони містять необ'єктивні чи некоректні формулювання.

6.3.2 Що означає «надмірний»?

181. У GDPR немає визначення терміну «надмірний». З одного боку, формулювання «зокрема, через їхній повторюваний характер» у статті 12(5) GDPR дозволяє зробити висновок, що основний сценарій застосування цього обмеження щодо статті 15 GDPR пов'язаний з кількістю запитів суб'єкта даних на отримання права на доступ. З іншого боку, вищезгадане формулювання показує, що інші причини, які можуть спричинити надмірність, не виключаються *апріорі*.

182. Безумовно, відповідно до статті 15(3) GDPR щодо права на отримання копії, суб'єкт даних може подати більше одного запиту до контролера[101]. У випадку запитів, які потенційно можуть бути розцінені як надмірні, оцінка «надмірності» залежить від аналізу, проведеного контролером, та специфіки сектору, в якому він працює.

183. У випадку наступних запитів необхідно оцінити, чи був перевищений поріг обґрунтованих інтервалів (див. преамбулу 63). Контролери повинні ретельно враховувати конкретні обставини кожного випадку.

184. Наприклад, у випадку із соціальними мережами зміни в наборі даних можна очікувати через коротші проміжки часу, ніж у випадку із земельними кадастрами або центральними реєстрами компаній. У випадку з діловими партнерами слід враховувати частоту контактів з клієнтом. Відповідно, «обґрунтовані інтервали», протягом яких суб'єкти даних можуть знову скористатися своїм правом на доступ, також відрізняються. Чим частіше відбуваються зміни в базі даних контролера, тим частіше суб'єктам даних може бути дозволено запитувати доступ до своїх персональних даних, і це не буде надмірним. З іншого боку, другий запит того самого суб'єкта даних за певних обставин може вважатися повторним.

185. Приймаючи рішення про те, чи минув відповідний проміжок часу, контролери повинні враховувати наступне у світлі обґрунтованих очікувань суб'єкта даних:

- як часто змінюються дані — чи малоймовірно, що інформація змінилася між запитами? Якщо пул даних очевидно не підлягає іншій обробці, окрім зберігання, і суб'єкт даних знає про це, наприклад, через попередній запит на отримання права на доступ, це може свідчити про надмірність запиту;
- характер даних — це може включати інформацію про те, чи є вони особливо конфіденційними;
- цілі обробки — вони можуть включати інформацію про те, чи може обробка спричинити шкоду (збитки) запитувачу, якщо вона буде розкрита;

[101] Відповідно до другого речення статті 15(3), контролер може стягувати обґрунтовану плату за додаткові запитувані копії.

- чи стосуються наступні запити того самого типу інформації або діяльності з обробки, чи різних[102].

Приклад 39 (столяр): Суб'єкт даних подає запити на отримання доступу до даних **кожні два місяці** столяру, який виготовив для нього стіл. На перший запит столяр відповів повністю. При вирішенні питання про те, чи минув обґрунтований проміжок часу, слід враховувати, що столяр лише час від часу (перший абзац вище), а не в рамках своєї основної діяльності, обробляє та збирає персональні дані, і ще менш імовірно, що столяр часто надає послуги одному й тому ж суб'єкту даних. Дійсно, у цій справі столяр не надав більше однієї послуги суб'єкту даних, що робить малоймовірним, що в наборі даних про суб'єкта даних відбулися зміни. Зокрема, враховуючи характер та обсяг оброблених персональних даних, ризики, пов'язані з обробкою, можна вважати низькими (другий абзац вище), наприклад, мета обробки (виставлення рахунків та дотримання зобов'язань щодо ведення обліку) навряд чи може завдати шкоди суб'єкту даних (третій абзац вище). Крім того, запит стосується тієї ж інформації, що й попередній запит (четвертий абзац вище). Як наслідок, такі запити можуть вважатися надмірними через їхню повторюваність.

Приклад 40 (соціальна мережа): Платформа соціальних мереж, основним видом діяльності якої є збір та/або обробка персональних даних суб'єкта даних, здійснює широкомасштабну складну та безперервну діяльність з обробки. Суб'єкт даних, який користується послугами платформи, подає запити на отримання доступу **кожні три місяці**. У цьому випадку дуже ймовірні часті зміни персональних даних, що стосуються суб'єкта даних (перший абзац вище), широкий спектр зібраних даних включає передбачувані конфіденційні персональні дані (другий абзац вище), які обробляються з метою показу суб'єкту даних релевантного контенту та учасників мережі (третій абзац вище). Запити на отримання доступу кожні три місяці — за цих обставин — у цілому не можуть вважатися надмірними через повторюваність.

Приклад 41 (кредитні агентства): Як і у випадку із соціальними мережами, не можна виключати, що зміни відповідних даних, які зберігаються кредитними агентствами, відбуватимуться зі значно меншими інтервалами, ніж в інших сферах (перший абзац вище). Це пов'язано з численними факторами, про які суб'єкт даних, як особа зі сторони, зазвичай не знає через складність бізнес-моделі. Тому відповідь на питання про те, які типи даних були зібрані контролером для розрахунку значення балів і які з них наразі включені в розрахунок, може надати лише сама кредитне агентство. Крім того, обробка даних через кредитні агентства та отримане в результаті значення рейтингу може мати далекосяжні наслідки для суб'єкта даних щодо запланованих юридичних операцій, таких як укладення договорів купівлі-продажу, оренди або лізингу (третій абзац вище).

[102] Якщо наступний запит стосується того ж типу інформації за обсягом ТА часом, це не питання надмірності, а питання запиту на додаткову копію, див. розділ 2.2.2.2.

Загалом неможливо визначити конкретний проміжок часу, протягом якого подання наступного запиту на отримання доступу може вважатися надмірним відповідно до другого речення статті 12(5) GDPR. Швидше за все, потрібно розглядати обставини конкретної справи в цілому. Однак, враховуючи важливість обробки даних для повсякденного життя суб'єктів даних, можна припустити, що **річний** інтервал між наданням інформації на безоплатній основі в будь-якому випадку буде занадто великим для того, щоб запит вважався надмірним. Якщо запит подається протягом дуже короткого проміжку часу, вирішальним фактором має бути те, чи має суб'єкт даних підстави вважати, що інформація або обробка змінилися з моменту останнього запиту. Зокрема, якщо суб'єкт даних здійснив фінансову операцію, наприклад, взяв кредит, він повинен мати право вимагати доступ до кредитної інформації, навіть якщо такий запит був поданий і відповідь на нього була надана незадовго до цього.

186. Якщо є можливість легко надати інформацію електронними засобами або шляхом віддаленого доступу до захищеної системи, тобто виконання таких запитів фактично не обтяжує контролера, навряд чи подальші запити можна вважати надмірними.

187. Якщо запит перетинається з попереднім запитом, такий запит, як правило, можна вважати надмірним, якщо і тою мірою, у якій він охоплює ту саму інформацію або діяльність з обробки, а попередній запит ще не виконаний контролером без досягнення стану «невиправданої затримки» (див. статтю 12(3) GDPR). На практиці, як наслідок, обидва запити можуть бути об'єднані.

188. Той факт, що контролеру знадобиться багато часу та зусиль, щоб надати інформацію або її копію суб'єкту даних, сам по собі не може зробити запит надмірним[103]. Велика кількість операцій з обробки зазвичай передбачає більші зусилля при виконанні запитів на отримання доступу. Однак, як зазначалося вище, за певних обставин запити можуть вважатися надмірними з інших причин, ніж їх повторюваний характер. На думку EDPB, це стосується, зокрема, випадків зловживання статтею 15 GDPR, тобто випадків, коли суб'єкти даних надмірно використовують право на доступ з єдиним наміром завдати шкоди або збитків контролеру.

189. З огляду на це, запит не слід вважати надмірним на тій підставі, що:

- суб'єкт даних не надає жодних причин для запиту або контролер вважає запит безпідставним;
- суб'єкт даних використовує неналежну або неввічливу мову;
- суб'єкт даних має намір використовувати дані для подання подальших претензій до контролера.[104]

190. З іншого боку, запит може бути визнаний надмірним, наприклад, якщо:

[103] Перевірка на обґрунтованість не проводиться, див. вище п. 166.

[104] Це не обмежує будь-яке застосовне національне законодавство, яке відповідає вимогам статті 23 GDPR, див. главу 6.4.

- фізична особа подає запит, але водночас пропонує відкликати його в обмін на певну вигоду від контролера, або
- запит має злий умисел і використовується для переслідування контролера або його працівників без жодних інших цілей, окрім як спричинити збої в роботі, наприклад, на підставі того, що:
    - особа прямо заявила в самому запиті або в інших повідомленнях, що вона має намір спричинити збій і ніщо інше; або
    - особа систематично надсилає контролеру різні запити в рамках кампанії, наприклад, раз на тиждень, з наміром і результатом спричинити збій у роботі[105].

6.3.3 Наслідки

191. У разі явно необґрунтованого або надмірного запиту на отримання права на доступ контролери можуть, відповідно до статті 12(5) GDPR, або стягнути обґрунтовану плату (з урахуванням адміністративних витрат на надання інформації чи повідомлення або вчинення запитуваних дій), або відмовити у задоволенні запиту.

192. EDPB зазначає, що, з одного боку, контролери, як правило, не зобов'язані стягувати обґрунтовану плату перед тим, як відмовити у виконанні запиту. З іншого боку, вони також не є повністю вільними у виборі між двома альтернативами. Фактично, контролери повинні приймати адекватне рішення залежно від конкретних обставин справи. У той час, як навряд чи можна уявити, що стягнення обґрунтованої плати є прийнятним заходом у випадку явно необґрунтованих запитів, для надмірних запитів — відповідно до принципу прозорості — часто буде більш доцільним стягувати плату як компенсацію адміністративних витрат, які спричиняють повторні запити.

193. Контролери повинні довести явно необґрунтований або надмірний характер запиту (третє речення статті 12(5) GDPR). Тому рекомендується забезпечити належне документування фактів, що лежать в основі запиту. Відповідно до статті 12(4) GDPR, якщо контролери відмовляються повністю або частково задовольнити запит на отримання доступу, вони повинні невідкладно, але не пізніше одного місяця з моменту отримання запиту, повідомити суб'єкта даних про:

    - причину відмови;
    - право подати скаргу до наглядового органу;
    - можливість звернутися за судовим захистом.

194. Перш ніж стягувати обґрунтовану плату на підставі статті 12(5) GDPR, контролери повинні повідомити суб'єктам даних про свій намір. Останні повинні вирішити, чи будуть вони відкликати запит, щоб уникнути стягнення плати.

[105] «Систематичне надсилання в рамках кампанії» означає, що запити, які можна було б легко об'єднати в один, штучно розбиваються суб'єктом даних не на кілька, а на багато окремих частин з явним наміром спричинити збої в роботі.

195. Необґрунтовані відхилення запитів на отримання права на доступ можуть розглядатися як порушення прав суб'єктів даних відповідно до статей 12-22 GDPR, а, отже, можуть бути підставою для застосування компетентними наглядовими органами коригувальних повноважень, включаючи адміністративні штрафи на підставі статті 83(5)(b) GDPR. Якщо суб'єкти даних вважають, що відбулося порушення їхніх прав суб'єкта даних, вони мають право подати скаргу на підставі статті 77 GDPR.

6.4 Можливі обмеження в законодавстві Союзу або держав-членів на підставі статті 23 GDPR та відступи від неї

196. Обсяг зобов'язань та прав, передбачених статтею 15 GDPR, може бути обмежений за допомогою законодавчих заходів у законодавстві Союзу або держав-членів[106].

197. Контролери, які планують покладатися на обмеження, засноване на національному законодавстві, повинні ретельно перевірити вимоги відповідного положення національного законодавства. Крім того, важливо зазначити, що обмеження права на доступ у законодавстві держав-членів (або Союзу), які ґрунтуються на статті 23 GDPR, повинні суворо відповідати умовам, викладеним у цьому положенні. EDPB випустила Настанови 10/2020 щодо обмежень, передбачених статтею 23 GDPR, з подальшими поясненнями із цього приводу. Що стосується права на доступ, EDPB нагадує, що контролери повинні зняти обмеження, як тільки обставини, що їх виправдовують, більше не будуть застосовуватися[107].

198. Законодавчі заходи, які стосуються обмежень, передбачених статтею 23 GDPR, можуть також передбачати, що реалізація права відкладається в часі, що право реалізується частково або обмежується певними категоріями даних або що право може бути реалізоване опосередковано через незалежний наглядовий орган[108].

---

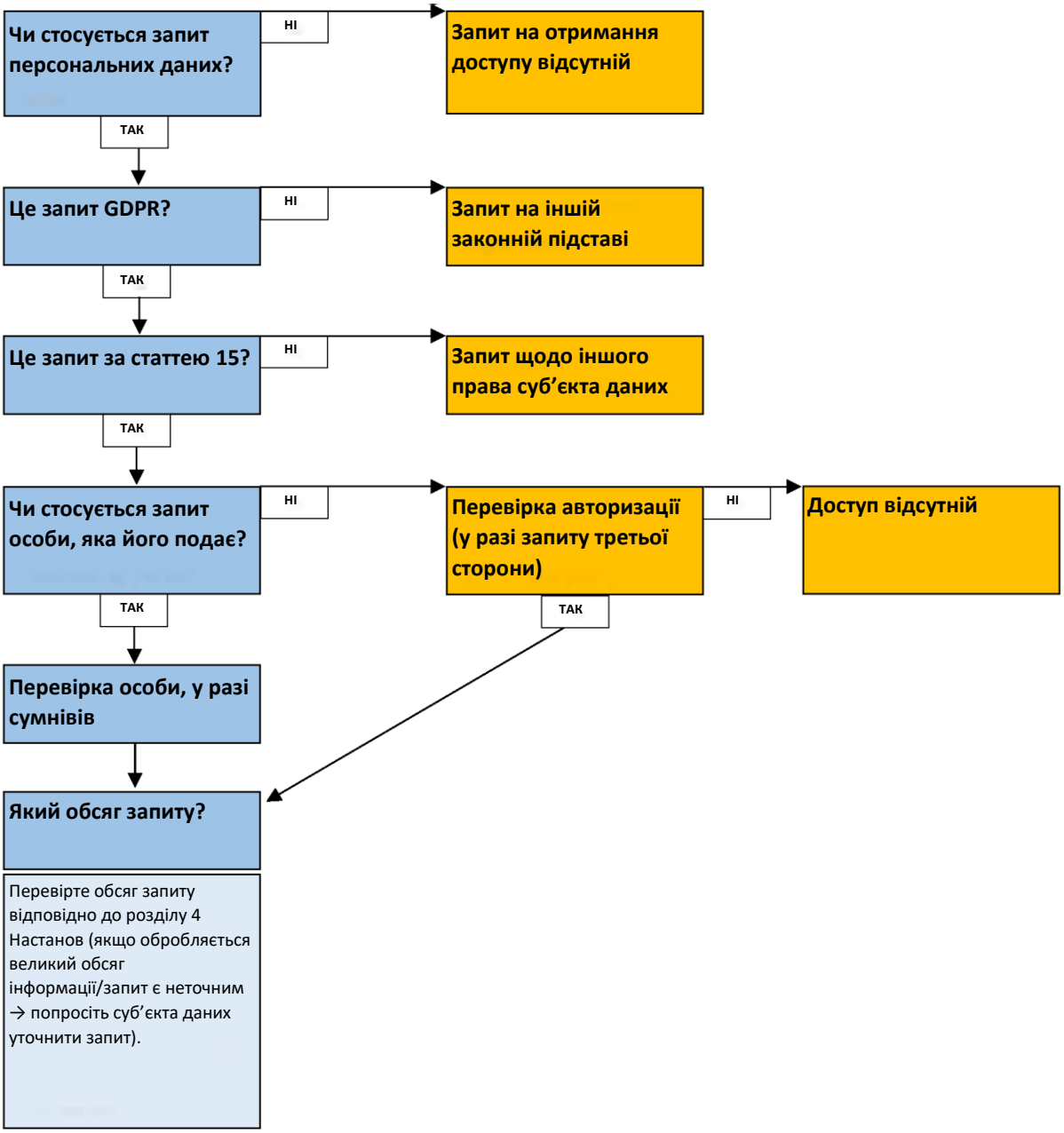
[106] Див. для прикладу статті 32-37 Федерального закону Німеччини про захист даних (BDSG), статті 16 і 17 Закону Норвегії про персональні дані та главу 5 Закону Швеції про захист даних.

[107] Пункт 76 Настанов 10/2020 щодо обмежень, передбачених статтею 23 GDPR, версія 2.0, прийнята 13 жовтня 2021 року.

[108] Пункт 12 Настанов 10/2020 щодо обмежень, передбачених статтею 23 GDPR, версія 2.0, прийнята 13 жовтня 2021 року. Наприклад, стаття 34(3) Федерального закону про захист даних Німеччини передбачає, що якщо державний орган не надає інформацію суб'єкту даних на запит про надання права на доступ через певні обмеження, така інформація надається федеральному наглядовому органу на запит суб'єкта даних, якщо тільки відповідальний вищий федеральний орган (органу, до якого надійшов запит) не визначить у кожному конкретному випадку, що це загрожуватиме безпеці Федерації або федеративної землі. Кодекс про захист персональних даних Італії (DPCode) передбачає опосередкований доступ (через орган влади) у випадку, якщо доступ може негативно вплинути на низку інтересів (наприклад, інтерес протидії відмиванню грошей), див. статтю Кодексу про захист персональних даних Італії.

ДОДАТОК – БЛОК-СХЕМА

Крок 1: Як інтерпретувати та оцінювати запит?



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

Крок 2: Як відповісти на запит (1)?

3 компоненти права на доступ (структура статті 15)		
Підтвердження того, чи обробляються персональні дані	Доступ до персональних даних	Додаткова інформація про цілі, одержувачів тощо (стаття 15(1)(a)-(h))

Крок 2: Як відповісти на запит (2)?

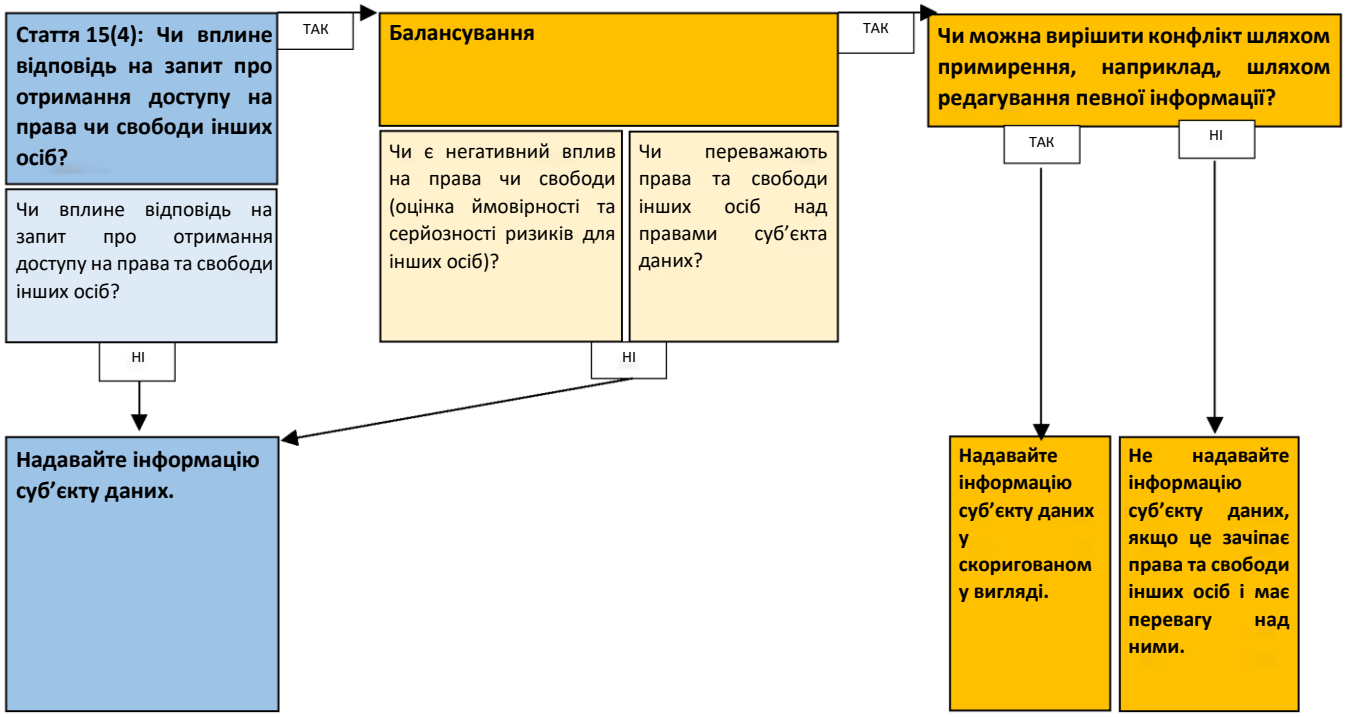
Вжити відповідних заходів			
Стаття 12(1): стисла, прозора, зрозуміла, доступна форма	Стаття 12(2): сприяти здійсненню права на доступ до інформації		
Обирайте між різними способами	Надати копію, якщо не узгоджено інше (стаття 15(3))	Використовуйте багаторівневий підхід, якщо це доцільно (найбільш актуально в онлайн-контексті)	Строки — без невиправданих затримок, у будь-якому випадку протягом одного місяця (у виняткових випадках — продовження на два місяці) (стаття 12(3)).

Крок 2: Як відповісти на запит (3)?

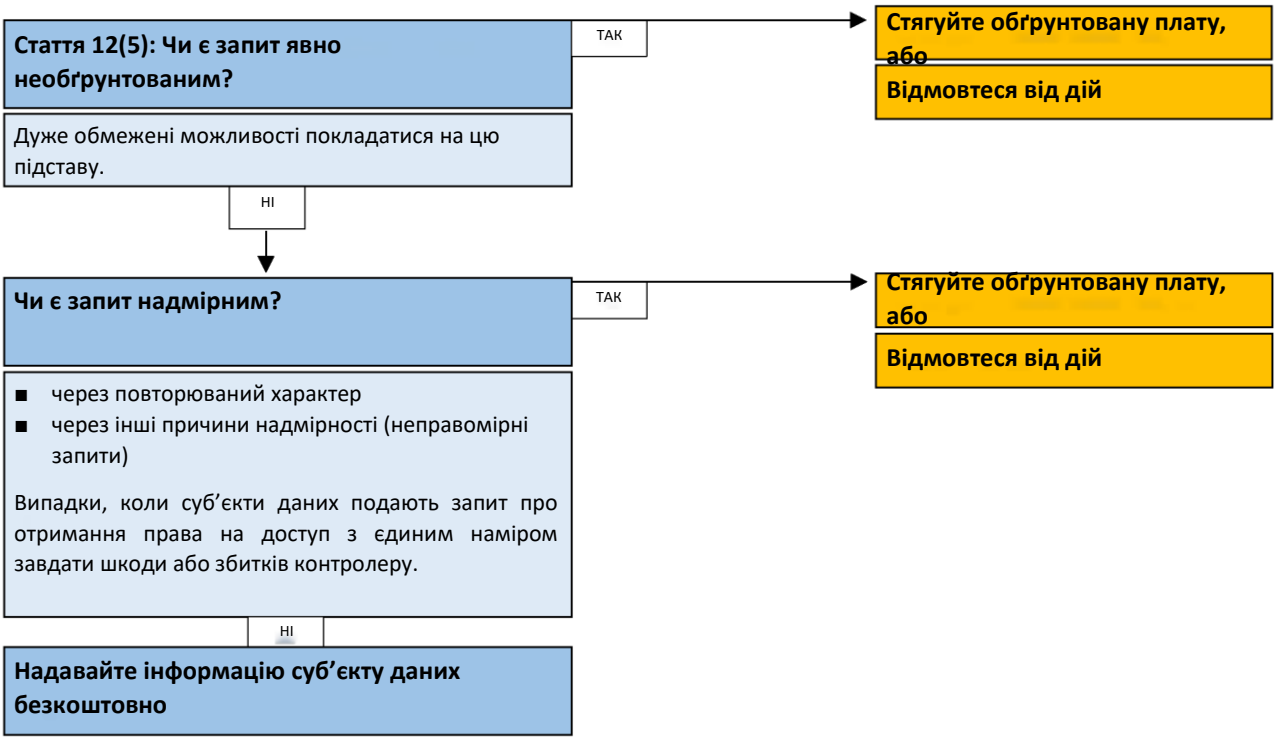
Як контролер може отримати всі дані про суб'єкта даних?			
Визначте критерії пошуку — на основі інформації, наданої суб'єктом даних, іншої інформації, яку має контролер про суб'єкта даних, та факторів, за якими структуровані дані (наприклад, номер клієнта, IP-адреси, професійна назва, родинні зв'язки тощо).	Визначте всі технічні функції, які можуть бути доступні для вилучення даних.	Шукайте в усіх відповідних IT- та не IT-системах зберігання даних.	Зберігайте, витягуйте або іншим чином збирайте дані, які стосуються суб'єкта даних, у спосіб, який повністю відображає обробку, тобто включає всі персональні дані, що стосуються суб'єкта даних, і дозволяє суб'єкту даних знати про обробку та перевіряти її законність. Отримання інформації може здійснюватися в кожному конкретному випадку або, коли це доцільно, за допомогою інструмента забезпечення конфіденційності, вже впровадженого контролером.

Прийнято

Крок 3: Перевірка лімітів та обмежень (1)



Крок 3: Перевірка лімітів та обмежень (2)



Прийнято