# ПРАВА СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ ВІДПОВІДНО ДО GDPR

1. Право бути поінформованим.
2. Право на виправлення.
3. Право на видалення даних.
4. Право на обмеження обробки.
5. Право на мобільність даних.
6. Право на заперечення.
7. Право на подання скарги до контролюючого органу.
8. Право на ефективний засіб судового захисту.

## 1. Право бути поінформованим.

Необхідна прозорість щодо збору та використання даних, щоб дозволити громадянам ЄС реалізувати своє право на захист персональних даних. Таким чином, Загальний регламент захисту даних (GDPR) надає особам право отримувати інформацію про збір і використання їхніх персональних даних, що призводить до різноманітних зобов'язань щодо інформації з боку контролера.

Закон розрізняє два випадки: з одного боку, якщо персональні дані отримані безпосередньо від суб'єкта даних (ст. 13 GDPR), а з іншого боку, якщо це не так (ст. 14 GDPR). ).

Якщо дані отримані безпосередньо, особа має бути негайно проінформована, тобто під час отримання даних. З точки зору змісту, зобов'язання контролера щодо інформування включає його особу, контактні дані уповноваженого із захисту даних (якщо є), цілі обробки та правову основу, будь-які законні інтереси, які переслідуються, одержувачів під час передачі персональних даних та будь-який намір передавати персональні дані в треті країни. Крім того, право бути поінформованим також включає інформацію про тривалість зберігання, права суб'єкта даних, можливість відкликати згоду,

право подати скаргу до органів влади та чи є надання персональних даних законом або договірна вимога. Крім того, суб’єкт даних повинен бути проінформований про будь-які автоматизовані дії з прийняття рішень, включаючи створення профілю. Лише якщо суб’єкт даних уже знає наведену вище інформацію, її не потрібно надавати.

Якщо персональні дані не отримані від суб’єкта даних, йому або їй необхідно надати інформацію протягом розумного періоду часу, але не пізніше ніж через місяць. У випадках, коли зібрана інформація використовується для безпосереднього зв’язку із суб’єктом даних, він або вона має право отримати інформацію одразу після звернення. Що стосується вмісту, контролер повинен надати таку саму конкретну інформацію, якби персональні дані були отримані безпосередньо від суб’єкта даних. Єдиним винятком є інформація про будь-які зобов’язання щодо надання персональних даних, оскільки контролер не має повноважень приймати рішення в цьому випадку. Крім того, контролер зобов’язаний повідомити, з яких джерел походять персональні дані та чи були вони загальнодоступними. Суб’єкт даних має право на отримання інформації у точній, прозорій, зрозумілій та легкодоступній формі. Зобов'язання щодо інформування може бути виконано в письмовій або електронній формі. Чітко зазначено, що так звані «стандартизовані символи зображення» також можуть використовуватися для того, щоб передати значущий огляд передбачуваної обробки в легкій для розуміння, зрозумілій і зрозумілій формі.

У випадку, якщо персональні дані не збираються від суб’єкта даних, у виняткових випадках немає зобов’язання інформувати. Це стосується випадків, коли надання інформації є неможливим або невиправдано дорогим, збирання та/або передача вимагається законом, або якщо дані повинні залишатися конфіденційними через професійну таємницю чи інші законні зобов’язання щодо таємниці.

## 2. Право на виправлення.

Відповідно до статті 16 GDPR особи мають право на виправлення неточних персональних даних. Особа також може отримати неповні персональні дані, хоча це залежатиме від цілей обробки. Це може передбачати надання додаткової заяви до неповних даних. Це право тісно пов'язане з принципом точності UDPR (стаття 5(1)(d)). Однак, хоча ви, можливо, вже вжили заходів, щоб переконатися, що персональні дані були точними, коли ви їх отримали, це право накладає конкретне зобов'язання переглянути точність на запит. Якщо ви отримуєте запит на виправлення, ви повинні вжити розумних заходів, щоб переконатися, що дані точні, і виправити дані, якщо це необхідно. Ви повинні взяти до уваги аргументи та докази, надані суб'єктом даних. Які кроки є розумними, залежатиме, зокрема, від характеру персональних даних і того, для чого вони будуть використовуватися. Чим важливіше, щоб персональні дані були точними, тим більше зусиль вам слід докласти, щоб перевірити їх точність і, якщо необхідно, вжити заходів для їх виправлення. Наприклад, вам слід докладати більше зусиль, щоб виправити неточні персональні дані, якщо вони використовуються для прийняття важливих рішень, які вплинуть на особу чи інших осіб, а не на тривіальні. Ви також можете взяти до уваги будь-які кроки, які ви вже вжили для перевірки точності даних до оскарження суб'єктом даних. GDPR не дає визначення терміну «точність». Проте в Законі про захист даних 2018 року (DPA 2018) зазначено, що персональні дані є неточними, якщо вони неправильні або вводять в оману щодо будь-якого факту. Визначення того, чи є персональні дані неточними, може бути складнішим, якщо дані стосуються помилки, яку згодом було виправлено. Можна стверджувати, що запис про помилку сам по собі точний і його слід зберігати. За таких обставин факт допущення помилки та правильна інформація також повинні бути включені до даних особи.

Згідно зі статтею 18 особа має право вимагати обмеження обробки своїх персональних даних, якщо вона заперечує їх точність, а ви їх перевіряєте. Як правило, ви повинні обмежити обробку відповідних персональних даних, поки

ви перевіряєте їх точність, незалежно від того, скористалася особа своїм правом на обмеження чи ні. Для отримання додаткової інформації перегляньте наші вказівки щодо права на обмеження.

Якщо застосовується виняток, ви можете відмовитися виконувати заперечення (повністю або частково). Не всі звільнення застосовуються однаково, тому вам слід уважно розглянути кожне звільнення, щоб побачити, як воно стосується конкретного запиту. Для отримання додаткової інформації, будь ласка, перегляньте наші вказівки щодо винятків.

Включення слова «явно» означає, що має бути очевидна або чітка якість необґрунтованості. Слід враховувати конкретну ситуацію та те, чи справді особа хоче скористатися своїми правами. Якщо це так, малоймовірно, що запит буде явно необґрунтованим.

### 3. Право бути забутим у кіберсередовищі.

Право бути забутим міститься в пунктах 65 і 66 і статті 17 GDPR. У ньому сказано: «Суб'єкт даних має право домагатися від контролера видалення персональних даних, що стосуються його чи неї, без невиправданої затримки, а контролер має зобов'язання видалити персональні дані без невиправданої затримки», якщо одна з кількох умов застосовується. «Невиправданою затримкою» вважається близько місяця. Ви також повинні вжити розумних заходів, щоб переконатися, що особа, яка вимагає видалення, справді є суб'єктом даних.

Право бути забутим узгоджується з правом людей на доступ до їх особистої інформації в статті 15. Право контролювати свої дані є безглуздим, якщо люди не можуть вжити заходів, коли вони більше не погоджуються на обробку, коли в даних є значні помилки або якщо вони вважають, що інформація зберігається без потреби. У цих випадках особа може вимагати видалення даних. Але це не абсолютне право. Якби це було так, критики, які стверджують, що право бути забутим означає не що інше, як переписування

історії, мали б рацію. Таким чином, GDPR проходить тонку межу щодо стирання даних.

У статті 17 GDPR викладено конкретні обставини, за яких застосовується право бути забутим. Фізична особа має право на видалення своїх персональних даних, якщо:

Особисті дані більше не потрібні для мети, для якої організація їх спочатку збирала або обробляла.

Організація покладається на згоду особи як законну основу для обробки даних, і ця особа відкликає свою згоду.

Організація покладається на законні інтереси як виправдання для обробки даних особи, особа заперечує проти такої обробки, і для організації немає переважаючого законного інтересу продовжувати обробку.

Організація обробляє персональні дані для цілей прямого маркетингу, і особа заперечує проти такої обробки.

Організація незаконно обробляла персональні дані фізичної особи.

Організація повинна видалити персональні дані, щоб виконати юридичне рішення чи зобов’язання.

Організація обробила персональні дані дитини, щоб запропонувати свої послуги інформаційного суспільства.

Проте право організації обробляти чиїсь дані може переважити право бути забутим. Ось причини, наведені в GDPR, які переважають право на видалення:

Дані використовуються для реалізації права на свободу вираження поглядів та інформації.

Дані використовуються для виконання правової постанови чи зобов’язання.

Дані використовуються для виконання завдання, яке виконується в суспільних інтересах або під час виконання офіційних повноважень організації.

Дані, що обробляються, необхідні для цілей охорони здоров’я та служать інтересам суспільства.

Дані, що обробляються, необхідні для здійснення профілактичної або професійної медицини. Це стосується лише випадків, коли дані обробляються медичним працівником, який зобов’язаний зберігати професійну таємницю.

Дані являють собою важливу інформацію, яка служить суспільним інтересам, науковим дослідженням, історичним дослідженням або статистичним цілям і де видалення даних може зашкодити або призупинити прогрес у досягненні мети обробки.

Дані використовуються для встановлення правового захисту або для здійснення інших правових вимог.

Крім того, організація може вимагати «розумну плату» або відхилити запит на видалення персональних даних, якщо організація може виправдати, що запит був необґрунтованим або надмірним.

Як бачите, у грі діє багато змінних, і кожен запит потрібно буде оцінювати окремо. Додайте до цього технічне навантаження щодо відстеження всіх місць, де зберігаються або обробляються персональні дані особи, і легко зрозуміти, чому нові права конфіденційності GDPR можуть бути значним тягарем для дотримання вимог для деяких організацій.

GDPR не визначає, що передбачає дійсний запит на видалення. Особа може подати запит на видалення в усній або письмовій формі. Цей запит також можна надіслати будь-якому члену вашої організації, а не лише вказаній контактній особі. За умови, що запит відповідає наведеним вище умовам, він є дійсним, навіть якщо в ньому не йдеться про «Запит на видалення», «Право бути забутим», статтю 17 або GDPR.

Це може створити проблему для організації, оскільки будь-який працівник може отримати дійсний усний запит. Нижче наведено зразок форми запиту «Право на видалення», яка може допомогти вам спростити процес. Зауважте, що це лише шаблон, який можна змінити відповідно до потреб вашої організації.

## 4. Право на обмеження обробки

Суб’єкт даних може вимагати від контролера обмеження обробки персональних даних, що стосуються його чи неї.

Обмеження обробки означає, що, окрім зберігання, персональні дані, на які поширюється обмеження, можуть лише оброблятися

- за згодою суб’єкта даних
- для встановлення, здійснення або захисту правових вимог
- для захисту прав іншої фізичної чи юридичної особи або
- з міркувань важливого суспільного інтересу Союзу або держави-члена.

Право на обмеження існує в таких випадках:

- Суб’єкт даних оскаржує точність персональних даних. У таких випадках обробка буде обмежена на період, який дозволить контролеру перевірити точність персональних даних.
- Обробка є незаконною, але суб’єкт даних виступає проти видалення персональних даних і натомість вимагає обмеження їх використання.
- Контролеру більше не потрібні персональні дані для цілей обробки, але вони потрібні суб’єкту даних для встановлення, здійснення або захисту правових вимог.
- Суб’єкт даних заперечив проти обробки персональних даних для цілей, відмінних від прямого маркетингу, і очікує перевірки того, чи законні підстави контролера переважають над підставами суб’єкта даних.
- Якщо обробку було обмежено, контролер повинен повідомити суб’єкта даних до того, як обмеження буде знято.

Обробку можна обмежити, наприклад, передавши дані в іншу систему обробки, заборонивши користувачам доступ до даних або видаливши опубліковані дані з веб-сайту.

Контролер повинен відповісти суб’єкту даних без невиправданої затримки та не пізніше одного місяця з моменту отримання запиту. У відповіді контролер зазначає заходи, вжиті ним за запитом.

Якщо запитів багато або складні, контролер може відповісти, що йому потрібно більше часу для їх обробки. У таких випадках термін може бути продовжено максимум на два місяці. Для продовження необхідно надати обґрунтування.

Якщо контролер відхиляє запит суб’єкта даних, він повинен повідомити суб’єкта даних про це протягом одного місяця з моменту отримання запиту. Відмова має бути обґрунтованою для суб’єкта даних. Крім того, контролер також повинен поінформувати суб’єкта даних про можливість подання скарги до наглядового органу та наявність засобів судового захисту.

Якщо запити суб’єкта даних щодо обмеження є явно необґрунтованими або надмірними, контролер може або стягнути з суб’єкта даних розумну плату, або відхилити запит.

Запити можуть вважатися явно необґрунтованими або надмірними, особливо якщо вони надходять неодноразово. Контролер несе тягар демонстрації явно необґрунтованого або надмірного характеру запиту.

При визначенні суми можливого збору необхідно враховувати адміністративні витрати, пов’язані з наданням інформації чи повідомлень або виконанням запитуваного заходу.

Контролер оцінює, чи виконуються умови для обмеження обробки даних. Якщо контролер виявляє, що право на обмеження обробки не застосовується, він має право відхилити запит, а суб’єкт даних може передати справу Уповноваженому із захисту даних.

Якщо запити суб’єкта даних є явно необґрунтованими або надмірними, контролер може або відхилити запит, або стягнути розумну плату за його виконання.

Якщо контролер відхиляє запит суб’єкта даних, він повинен повідомити суб’єкта даних про це протягом одного місяця з моменту отримання запиту.

Відмова має бути обґрунтованою для суб'єкта даних. Крім того, контролер також повинен поінформувати суб'єкта даних про можливість подання скарги Омбудсмену із захисту даних та наявність засобів судового захисту.

Крім того, можливе відступлення від права доступу до даних за певних умов у зв'язку з проведенням наукових чи історичних досліджень або підготовкою статистики. Додаткова інформація про відступи від прав суб'єктів даних

Якщо можливо, контролер повинен повідомити кожного одержувача, якому було розкрито персональні дані, про обмеження обробки. Контролер зобов'язаний повідомити суб'єкта даних про цих одержувачів, якщо цього вимагає суб'єкт даних.

Контролер повинен мати можливість підтвердити особу суб'єкта даних, який здійснює свої права на захист даних. Якщо у контролера є обґрунтовані сумніви щодо особи особи, яка звернулася із запитом, він може вимагати надання додаткової інформації, необхідної для підтвердження її особи.

GDPR не передбачає способів підтвердження особи суб'єкта даних. Багато контролерів уже мають відповідні процедури. Наприклад, контролер міг перевірити особу суб'єкта даних перед укладенням угоди або отриманням згоди на обробку. Потім ці персональні дані можуть бути використані для підтвердження особи суб'єкта даних також у зв'язку з виконанням прав суб'єкта даних.

Якщо контролер запитує додаткову інформацію для підтвердження особи суб'єкта даних, це не може призвести до необґрунтованих вимог або збору персональних даних, які не є актуальними чи необхідними.

Якщо контролер не може ідентифікувати суб'єкта даних, він повинен повідомити його про це, якщо це можливо.

Якщо контролер відхиляє запит суб'єкта даних через нездатність ідентифікувати суб'єкта даних, він повинен продемонструвати, що він не може підтвердити особу суб'єкта даних.

**5. Право на мобільність даних.**

Право на перенесення даних дає особам право отримувати персональні дані, які вони надали контролеру, у структурованому, широко використовуваному та машиночитаному форматі. Це також дає їм право вимагати, щоб контролер передавав ці дані безпосередньо іншому контролеру.

Право на перенесення даних застосовується лише тоді, коли:

- вашою законною підставою для обробки цієї інформації є згода або виконання контракту;
- ви виконуєте обробку автоматизованими засобами (тобто за винятком паперових файлів).

Інформація входить до сфери права на перенесення даних лише в тому випадку, якщо вона надала вам особисті дані особи.

Іноді особисті дані, надані вам особою, буде легко ідентифікувати (наприклад, її поштову адресу, ім'я користувача, вік). Однак значення «наданих» вам даних не обмежується цим. Це також персональні дані, отримані в результаті спостереження за діяльністю особи (наприклад, під час використання пристрою чи послуги).

Це може включати:

- історія використання веб-сайту або пошукових дій;
- трафік і дані про місцезнаходження; або
- «необроблені» дані, які обробляються підключеними об'єктами, такими як розумні лічильники та переносні пристрої.

Він не містить жодних додаткових даних, які ви створили на основі даних, наданих вам особою. Наприклад, якщо ви використовуєте надані ними дані для створення профілю користувача, ці дані не підпадають під дію переносимості даних.

Проте ви повинні зауважити, що якщо ці «припущення» або «похідні» дані є особистими даними, ви все одно повинні надати їх особі, якщо вона

надсилає запит на доступ до суб'єкта. Пам'ятаючи про це, якщо зрозуміло, що особа шукає доступ до передбачуваних/похідних даних у рамках ширшого запиту на перенесення, доцільно було б включити ці дані у свою відповідь.

Право на перенесення даних стосується лише персональних даних. Це означає, що воно не стосується справді анонімних даних. Проте дані під псевдонімом, які можна чітко пов'язати з особою (наприклад, якщо ця особа надає відповідний ідентифікатор), входять до сфери дії права.

Якщо запитувана інформація містить інформацію про інших осіб (наприклад, дані третіх сторін), вам потрібно розглянути, чи передача цих даних негативно вплине на права та свободи цих третіх сторін.

Загалом, надання даних третьої сторони особі, яка надсилає запит на перенесення, не повинно бути проблемою, якщо припустити, що запитувач надав ці дані вам у своїй інформації. Однак ви завжди повинні враховувати, чи це матиме негативний вплив на права та свободи третіх осіб, зокрема, коли ви передаєте дані безпосередньо іншому контролеру.

Якщо запитані дані були надані вам декількома суб'єктами даних (наприклад, спільний банківський рахунок), ви повинні бути впевнені, що всі сторони погоджуються на запит на перенесення. Це означає, що вам, можливо, доведеться отримати згоду від усіх залучених сторін.

Право на перенесення даних дає право фізичній особі:

- отримати копію своїх персональних даних; та/або
- передавати свої персональні дані від одного контролера до іншого контролера.

Фізичні особи мають право отримувати свої персональні дані та зберігати їх для подальшого особистого використання. Це дозволяє особі керувати та повторно використовувати свої персональні дані. Наприклад, особа хоче отримати свій список контактів із програми веб-пошти, щоб створити весільний список або зберегти свої дані в сховищі персональних даних.

Ви можете вибрати бажаний спосіб надання запитуваної інформації залежно від обсягу та складності запитуваних даних. У будь-якому випадку вам потрібно переконатися, що метод безпечний.

Особи мають право попросити вас безперешкодно передати їхні персональні дані безпосередньо іншому контролеру. Якщо це технічно можливо, ви повинні це зробити.

Ви повинні розглянути технічну можливість передачі на основі кожного запиту. Право на перенесення даних не створює для вас зобов'язання приймати або підтримувати системи обробки, які технічно сумісні з системами інших організацій.

Однак ви повинні прийняти розумний підхід, і це, як правило, не повинно створювати перешкоду для передачі.

Без перешкод означає, що ви не повинні встановлювати будь-які юридичні, технічні чи фінансові перешкоди, які уповільнюють або перешкоджають передачі персональних даних особі чи іншій організації.

Однак можуть існувати законні причини, чому ви не можете здійснити передачу. Наприклад, якщо передача негативно вплине на права та свободи інших осіб. Однак ви повинні обґрунтувати, чому ці причини є законними та чому вони не є «перешкодою» для передачі.

Якщо ви надаєте інформацію безпосередньо особі чи іншій організації у відповідь на запит щодо перенесення даних, ви не несете відповідальності за будь-яку подальшу обробку, виконану цією особою чи іншою організацією. Однак ви несете відповідальність за передачу даних і повинні вжити відповідних заходів, щоб гарантувати їх безпечну передачу до потрібного пункту призначення.

Якщо ви надаєте дані особі, можливо, вона зберігатиме інформацію в системі з меншим рівнем безпеки, ніж ваша власна. Тому ви повинні повідомити про це осіб, щоб вони могли вжити заходів для захисту інформації, яку вони отримали.

Вам також потрібно переконатися, що ви дотримуєтеся інших положень GDPR. Наприклад, хоча в рамках права на переносимість даних немає конкретного зобов'язання щодо перевірки та підтвердження якості даних, які ви передаєте, ви вже повинні вжити розумних заходів для забезпечення точності цих даних, щоб відповідати вимогам принцип точності GDPR.

### 6. Право на заперечення.

Ви маєте право заперечити проти певних типів обробки ваших персональних даних, якщо ця обробка здійснюється у зв'язку із завданнями:

- в суспільних інтересах,
- під офіційною владою, або
- в законних інтересах інших осіб.

Ви маєте більше права заперечувати проти обробки ваших персональних даних, якщо обробка стосується прямого маркетингу. Якщо контролер даних використовує ваші персональні дані з метою маркетингу чогось безпосередньо вам або профілювання для цілей прямого маркетингу, ви можете заперечити в будь-який час, і контролер даних повинен припинити обробку, як тільки він отримає ваше заперечення.

Ви також можете заперечити проти обробки ваших особистих даних для дослідницьких цілей, якщо обробка не потрібна для виконання завдання, яке виконується в суспільних інтересах.

Щоб заперечити проти обробки, ви повинні зв'язатися з контролером даних і вказати підстави для свого заперечення. Ці підстави мають стосуватися вашої конкретної ситуації. Якщо ви зробили обґрунтоване заперечення, контролер даних повинен припинити обробку ваших персональних даних, якщо тільки контролер даних не може надати вагомі законні причини для продовження обробки ваших даних. Контролери даних також можуть на законних підставах продовжувати обробляти ваші персональні дані, якщо це необхідно для певних видів правових вимог.

Якщо застосовується право на заперечення, контролери даних зобов’язані повідомити вас про це під час першого спілкування з вами. Якщо обробка здійснюється онлайн, контролери даних повинні запропонувати онлайн-метод для заперечення.

Ваші права щодо автоматизованого прийняття рішень, включаючи профілювання (стаття 22 GDPR)

Ви маєте право не підпадати під рішення, засноване виключно на автоматизованій обробці. Обробка є «автоматизованою», якщо вона виконується без втручання людини та має юридичні наслідки або суттєво впливає на вас.

Автоматизована обробка дозволена лише з вашої прямої згоди, якщо це необхідно для виконання контракту або якщо це дозволено законодавством Союзу чи держав-членів. У разі застосування одного з цих винятків повинні бути вжиті відповідні заходи для захисту ваших прав, свобод і законних інтересів. Це може включати право на людське втручання з боку контролера, право представити свою точку зору та право оскаржити рішення.

Якщо автоматизована обробка стосується спеціальних категорій персональних даних (викладених у наведених вище ключових визначеннях), обробка є законною лише тоді, коли ви дали свою чітку згоду на обробку або якщо це необхідно з міркувань значного суспільного інтересу.

## 7. Право на подання скарги до контролюючого органу.

Право на подання скарги до контролюючого органу

1. Без шкоди для будь-яких інших адміністративних або судових засобів правового захисту, кожен суб’єкт даних має право подати скаргу до наглядового органу, зокрема в державі-члені його або її постійного проживання, місця роботи або місця передбачуваного порушення. якщо суб’єкт даних вважає, що обробка персональних даних, що стосуються його чи неї, порушує цей Регламент.

2. Наглядовий орган, до якого було подано скаргу, інформує скаржника про хід і результати розгляду скарги, включаючи можливість судового захисту відповідно до статті 78.

Стаття 77(1) GDPR передбачає право суб'єкта даних подати скаргу до наглядового органу («SA») у разі порушення GDPR. Стаття 77(2) GDPR покладає на SA, до якого було подано скаргу, зобов'язання інформувати скаржника про хід і результати розгляду скарги. Обидві статті 77(1) і (2) GDPR застосовуються безпосередньо та не потребують перенесення в національне законодавство. Однак деталі процедури розгляду скарг регулюються законодавством держав-членів, яке має відповідати вимогам і цілям GDPR.[1] Багато SA надають форми, які гарантують, що скаржник включає всю відповідну інформацію, як запропоновано в останньому реченні пункту 141 GDPR.

(1) Право на офіційну скаргу

Згідно зі статтею 77(1) GDPR, кожен суб'єкт даних має право подати скаргу до SA, зокрема в державі-члені свого постійного проживання, місця роботи чи місця передбачуваного порушення, якщо суб'єкт даних вважає, що обробка пов'язаних з ними персональних даних порушує GDPR.

Без шкоди для будь-якого адміністративного чи судового захисту

Право на подання скарги згідно зі статтею 77(1) не обмежує будь-які інші доступні адміністративні чи судові засоби захисту. Наприклад, суб'єкт даних все ще може порушити судовий процес проти контролера або процесора (згідно зі статтею 79 GDPR) незалежно від того, чи була подана скарга до наглядового органу, одночасно чи незалежно.[2] Подання скарги до наглядового органу не впливає на прийнятність або дійсність інших засобів правового захисту.

CJEU: CJEU нещодавно роз'яснив, що «стаття 77(1), стаття 78(1) і стаття 79(1) Регламенту (ЄС) 2016/679 повинні тлумачитися як такі, що дозволяють засоби правового захисту, передбачені статтею 77(1) і статтю 78(1) цього Регламенту, з одного боку, і його статтю 79(1) з іншого, які мають виконуватися

одночасно та незалежно одна від одної. Це для держав-членів, у відповідно до принципу процесуальної автономії, щоб встановити детальні правила щодо взаємозв'язку між цими засобами правового захисту з метою забезпечення ефективного захисту прав, гарантованих цим регламентом, та послідовного та однорідного застосування його положень, а також права на ефективний засіб правового захисту в суді, як зазначено в статті 47 Хартії основних прав».

Рішення про те, чи обрати процедуру подання скарги чи інший засіб правового захисту, залежить від потерпілої особи та на нього можуть впливати аспекти практичності чи ефективності, окрім юридичних міркувань. Деякими з цих аспектів можуть бути судові витрати, процесуальна доцільність, наявність або відсутність процесуальних прав, включаючи право бути заслуханим протягом усього процесу.

Загальний регламент захисту даних (GDPR) надає суб'єктам даних право подати «скаргу» до наглядового органу. Всупереч тому, що стверджують деякі вчені, ми не вважаємо, що це право є простим «клопотанням» до влади, що дозволяє їй діяти чи ні відповідно до власних пріоритетів.

Крім буквального формулювання (закон говорить про «скаргу», а не про «клопотання»), є кілька елементів, які свідчать про те, що скарга зобов'язує орган вжити заходів і прийняти рішення щодо конкретних питань, порушених скаржником.

По-перше, захист персональних даних є фундаментальним правом особи, а право на сприятливе рішення через скаргу є одним із фундаментальних елементів забезпечення такого захисту. У GDPR є численні елементи, що підтверджують це тлумачення.

Щоб навести деякі з них, стаття 57(1)(f) вимагає, щоб наглядовий орган «розглядав скарги, подані суб'єктом даних», «розслідував, у належному обсязі, предмет скарги» та «інформував скаржника про хід і результати розслідування протягом розумного періоду». Буква закону зрозуміла. Після отримання будь-якої скарги наглядовий орган повинен вжити заходів, щоб прийняти будь-яке рішення, навіть якщо в кінцевому підсумку це буде відмова.

**8. Право на ефективний засіб судового захисту.**

Без шкоди для будь-яких інших адміністративних чи позасудових засобів правового захисту кожна фізична чи юридична особа має право на ефективний судовий захист проти юридично обов'язкового рішення наглядового органу щодо неї.

Без шкоди для будь-яких інших адміністративних або позасудових засобів правового захисту, кожен суб'єкт даних має право на ефективний судовий засіб правового захисту, якщо наглядовий орган, який є компетентним відповідно до статей 55 і 56, не розглядає скаргу або не інформує суб'єкта даних протягом три місяці про хід або результат розгляду скарги, поданої відповідно до статті 77.

Позови проти наглядового органу подаються в судах держави-члена, де засновано наглядовий орган.

Якщо провадження порушується проти рішення наглядового органу, якому передував висновок або рішення Правління в механізмі узгодженості, наглядовий орган передає цей висновок або рішення до суду.

**Список використаних джерел:**

1. Art. 78 GDPR. *Intersoft Consulting :* website. URL : https://gdpr-info.eu/art-78-gdpr/

2. Article 77 GDPR. *GDPR HUB :* website. URL : https://gdprhub.eu/Article_77_GDPR

3. Everything you need to know about the "Right to be forgotten". GDPREU *:* website. URL : https://gdpr.eu/right-to-be-forgotten/

4. Right to be Informed. URL : https://gdpr-info.eu/issues/right-to-be-informed/

5. Right to data portability *ICQ :* website. URL : https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-

portability/#:~:text=The%20right%20to%20data%20portability,way%2C%20without%20affecting%20its%20usability.

6. Right to rectification. *ICQ :* website. URL : https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification/

7. Right to restriction of processing. *Data Protection Ombudsman's Office :* website. URL : https://tietosuoja.fi/en/right-to-restriction-of-processing

8. The right to object to processing of personal data (Article 21 of the GDPR). *Your Data :* website. URL : https://www.dataprotection.ie/en/individuals/know-your-rights/right-object-processing-personal-data-article-21-gdpr