Міжнародні та регіональні стандарти у сфері охорони здоров'я і практика їх застосування

РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/679*

від 27 квітня 2016 р.

про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)

(Текст стосується ЄЕП)

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ І РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про функціонування Європейського Союзу, зокрема його ст. 16,

Беручи до уваги пропозицію Європейської Комісії,

Після передавання проекту законодавчого акта національним парламентам,

Беручи до уваги висновок Європейського економічно-соціального комітету**,

---

* Офіційний переклад, текст відредагований.

** ОВ С 229, 31.07.2012, с. 90.

Беручи до уваги висновок Комітету регіонів*,

Діючи згідно зі звичайною законодавчою процедурою**,

Оскільки:

1. Захист фізичних осіб під час опрацювання персональних даних є фундаментальним правом. Статтею 8 (1) Хартії фундаментальних прав Європейського Союзу («Хартія») і статтею 16 (1) Договору про функціонування Європейського Союзу (ДФЄС) встановлено, що кожна особа має право на захист своїх персональних даних.

2. Принципи і норми щодо захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних передбачають, незалежно від їхнього громадянства або місця проживання, дотримання їхніх фундаментальних прав і свобод, зокрема їхнього права на захист персональних даних. Цей Регламент спрямовано на сприяння формуванню простору свободи, безпеки і правосуддя, економічному союзу, соціально-економічному прогресові, зміцненню та конвергенції економік у межах внутрішнього ринку, підтриманню добробуту фізичних осіб.

3. Директиву Європейського Парламенту і Ради 95/46/ЄС*** спрямовано на гармонізацію захисту фундаментальних прав і свобод фізичних осіб під час опрацювання персональних даних і забезпечення вільного руху персональних даних між державами-членами.

4. Опрацювання персональних даних призначено для служіння людству. Право на захист персональних даних не є абсолютним правом; воно повинно розглядатися у зв'язку з його функцією у суспільстві та бути збалансованим з іншими фундаментальними правами, згідно з принципом пропорційності. У цьому Регламенті дотримано всі фундаментальні права та свободи і принципи, визнані у Хартії, як це передбачено в Договорах, зокрема, щодо поваги до приватного та сімейного життя, житла та спілкування, захисту персональних даних, свободи думки, совісті та віросповідання, свободи вияву поглядів і свободи інформації, свободи підприємництва, права на дієвий засіб правового захисту та справедливий суд, а також – культурного, релігійного та мовного різноманіття.

5. Економічна та соціальна інтеграція як результат функціонування внутрішнього ринку спричинила істотне зростання транскордонних потоків персональних даних. Зріс обмін персональними даними між публічними та приватними суб'єктами, в тому числі фізичними особами, асоціаціями та підприємствами на рівні Союзу. Відповідно до законодавства Союзу,

---

* ОВ С 391, 18.12.2012, с. 127.

** Позиція Європейського Парламенту від 12 березня 2014 р. (ще не опубліковано в Офіційному віснику) і позиція Ради в першому читанні від 8 квітня 2016 р. (ще не опубліковано в Офіційному віснику). Позиція Європейського Парламенту від 14 квітня 2016 р.

*** Директива Європейського Парламенту і Ради 95/46/ЄС від 24 жовтня 1995 р. про захист осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (ОВ L 281, 23.11.1995, с. 31).

національні органи держав-членів закликають до співпраці та обміну персональними даними для надання їм можливості виконувати свої обов'язки або завдання від імені органу в іншій державі-члені.

6. Стрімкий технологічний розвиток і глобалізація призводять до виникнення нових труднощів для захисту персональних даних. Масштаби збирання та спільного використання персональних даних суттєво зросли. Технології дають змогу як приватним компаніям, так і публічним органам користуватися персональними даними в безпрецедентних масштабах з метою реалізації своєї діяльності. Фізичні особи дедалі частіше надають доступ до персональної інформації для громадськості та в глобальному масштабі. Технології змінили як економіку, так і суспільне життя і повинні надалі стимулювати вільний рух персональних даних у межах Союзу та передавання їх до третіх країн і міжнародних організацій, забезпечуючи при цьому високий рівень захисту персональних даних.

7. Такі зміни вимагають міцних і більш узгоджених засад щодо захисту даних у Союзі, із запровадженням належного механізму виконання, враховуючи важливість формування довіри, що уможливить розвиток цифрової економіки на рівні внутрішнього ринку. Фізичні особи повинні мати контроль над власними персональними даними. Необхідно зміцнити правову та практичну визначеність для фізичних осіб, суб'єктів господарювання та органів публічної влади.

8. Якщо цим Регламентом передбачено уточнення або обмеження його норм законодавством держав-членів, у такому разі останні можуть, за необхідності узгоджувати і забезпечувати розуміння положень національного законодавства особами, на яких вони поширюються, інкорпорувати елементи цього Регламенту в своє національне законодавство.

9. Цілі та принципи Директиви 95/46/ЄС зберігають свою силу, проте це не запобігає фрагментації в процесі реалізації захисту даних у межах Союзу, правовій невизначеності чи широкому розповсюдженню громадської думки про існування значних ризиків для захисту фізичних осіб, зокрема у зв'язку з діяльністю онлайн. Відмінності в рівнях захисту прав і свобод фізичних осіб, зокрема права на захист персональних даних, у зв'язку з опрацюванням персональних даних у державах-членах можуть перешкоджати вільному переміщенню персональних даних усередині Союзу. Відповідно, такі відмінності можуть перешкоджати провадженню економічної діяльності на рівні Союзу, спотворювати конкуренцію та заважати органам влади виконувати свої обов'язки відповідно до законодавства Союзу. Така відмінність у рівнях захисту виникає внаслідок відмінностей у процедурі імплементації та застосування Директиви 95/46/ЄС.

10. Для забезпечення сталого та високого рівня захисту фізичних осіб й усунення перешкод для потоків персональних даних у межах Союзу у всіх державах-членах рівень захисту прав і свобод фізичних осіб у зв'язку з опрацюванням таких даних повинен бути однаковим. Необхідно забезпечити послідовне та однорідне застосування норм щодо захисту фунда-

ментальних прав і свобод фізичних осіб у зв'язку з опрацюванням персональних даних у всьому Союзі. Якщо опрацювання персональних даних здійснюють відповідно до встановлених законом зобов'язань, для задоволення суспільних інтересів або для виконання офіційних повноважень, покладених на контролера, державам-членам необхідно дозволити мати або запроваджувати національного законодавства положення, які більш детально уточнюватимуть застосування норм цього Регламенту. Разом із загальним і горизонтальним законодавством, що регулює питання захисту даних, за допомогою якого імплементують Директиву 95/46/ЄС, держави-члени мають декілька секторальних законів у сферах, що потребують уточнених положень. Цей Регламент також надає державам-членам простір для маневру в уточненні своїх норм, зокрема щодо опрацювання спеціальних категорій персональних даних («чутливих даних»). Відповідно, цей Регламент не виключає законодавство держави-члена у визначенні обставин особливих ситуацій опрацювання, зокрема в уточненні умов, за яких опрацювання персональних даних є правомірним.

11. Дієвий захист персональних даних у всьому Союзі вимагає зміцнення та детального опису прав суб'єктів даних і обов'язків осіб, які здійснюють опрацювання й ухвалюють рішення щодо опрацювання персональних даних, а також надання рівнозначних повноважень з моніторингу і забезпечення дотримання норм щодо захисту персональних даних і застосування відповідних санкцій за порушення прав у державах-членах.

12. Стаття 16 (2) ДФЄС уповноважує Європейський Парламент і Раду встановити норми щодо захисту фізичних осіб у зв'язку з опрацюванням персональних даних і норми про вільний рух персональних даних.

13. Для забезпечення послідовного рівня захисту фізичних осіб у всьому Союзі та запобігання виникненню розбіжностей, що ускладнюють вільний рух персональних даних у межах внутрішнього ринку, необхідно, щоб Регламент забезпечував правову визначеність і прозорість для суб'єктів господарювання, у тому числі мікропідприємств, малих і середніх підприємств, надавав фізичним особам у всіх державах-членах однаковий рівень прав і зобов'язань, що мають юридичну силу, та обов'язків для контролерів і операторів, забезпечував постійний моніторинг опрацювання персональних даних, належні санкції в усіх державах-членах, а також дієву співпрацю між наглядовими органами різних держав-членів. Належне функціонування внутрішнього ринку вимагає, щоб вільний рух персональних даних у всьому Союзі не було обмежено чи заборонено з причин, пов'язаних із захистом фізичних осіб у зв'язку з опрацюванням персональних даних. Щоб врахувати особливу ситуацію мікропідприємств, малих і середніх підприємств, для організацій з численністю штатних працівників менше 250 осіб цим Регламентом передбачено відступ у частині ведення обліку. Окрім того, установи та органи влади Союзу, держави-члени, а також їх наглядові органи закликають враховувати особливі потреби мікропідприємств, малих і середніх підприємств при застосуванні цього Регламенту.

Поняття мікропідприємств, малих і середніх підприємств повинно відповідати означенню, яке містять положення ст. 2 додатка до Рекомендації Комісії 2003/361/ЄС*.

14. Захист, передбачений цим Регламентом, поширюється на фізичних осіб, незалежно від їхнього громадянства чи місця проживання, під час опрацювання їхніх персональних даних. Цей Регламент не поширюється на опрацювання персональних даних юридичних осіб і, зокрема, підприємств, заснованих як юридичні особи, які містять інформацію про найменування, організаційно-правову форму юридичної особи і контактну інформацію юридичної особи.

15. Для запобігання виникненню серйозного ризику правопорушення захист фізичних осіб повинен бути технологічно нейтральним і незалежним від методів, які використовують. Захист фізичних осіб застосовують до опрацювання персональних даних за допомогою автоматизованих і ручних засобів, якщо персональні дані містяться в картотеці або призначені для внесення до неї. На файли або групи файлів, а також їх титульні сторінки, які не структуровано за спеціальними критеріями, чинність цього Регламенту не поширюється.

16. Цей Регламент не застосовують до питань захисту фундаментальних прав і свобод або вільного потоку персональних даних, пов'язаних з діяльністю поза межами законодавства Союзу, наприклад, з діяльністю щодо національної безпеки. Цей Регламент не застосовують до опрацювання персональних даних державами-членами у ході діяльності щодо спільної зовнішньої та безпекової політики Союзу.

17. Регламент Європейського Парламенту і Ради (ЄС) № 45/2001** застосовують до опрацювання персональних даних установами, органами, офісами та агентствами Союзу. Регламент (ЄС) № 45/2001 та інші нормативно-правові акти Союзу, застосовні до такого опрацювання персональних даних, необхідно адаптувати до принципів і норм, встановлених цим Регламентом і застосовних у зв'язку з ним. Для забезпечення міцних та узгоджених засад щодо захисту даних у Союзі необхідно здійснити адаптацію Регламенту (ЄС) № 45/2001 після адаптації цього Регламенту, що дозволяє його застосування одночасно із застосуванням цього Регламенту.

18. Цей Регламент не застосовують до опрацювання персональних даних фізичною особою у ході суто особистої або побутової діяльності, а, отже, жодним чином не пов'язаної з професійною чи комерційною діяльністю. Особисту або побутову діяльність може становити ведення кореспонденції та зберігання адрес, ведення соціальних мереж і онлайн-діяльності, роз-

---

* Рекомендація Комісії від 6 травня 2003 р. щодо означення мікропідприємств, малих і середніх підприємств (C(2003) 1422) (OB L 124, 20.05.2003, с. 36).

** Регламент Європейського Парламенту і Ради (ЄС) № 45/2001 від 18 грудня 2000 р. про захист осіб у зв'язку з опрацюванням персональних даних установами та органами Співтовариства і про вільний рух таких даних (OB L 8, 12.01.2001, с. 1).

початої у контексті такої діяльності. Проте цей Регламент застосовують до контролерів і операторів, які надають засоби для опрацювання персональних даних для такої особистої або побутової діяльності.

19. На захист фізичних осіб у зв'язку з опрацюванням персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування за скоєння кримінальних злочинів або для виконання кримінальних покарань, у тому числі захисту від або запобігання загрозам громадській безпеці та вільному руху таких даних, поширюється застосування спеціального нормативно-правового акта Союзу. Відповідно, цей Регламент не можна застосовувати до опрацювання даних для таких цілей. Проте питання щодо опрацювання персональних даних, яке здійснюють органи публічної влади, згідно з цим Регламентом, у разі їх використання для таких цілей, підлягає врегулюванню уточненим спеціальним нормативно-правовим актом Союзу, зокрема Директивою Європейського Парламенту і Ради (ЄС) 2016/680*. Держави-члени можуть доручити компетентним органам у значенні Директиви (ЄС) 2016/680 завдання, які необов'язково виконують для цілей запобігання, розслідування, виявлення або переслідування за скоєння кримінальних злочинів або для виконання кримінальних покарань, у тому числі захисту від або запобігання загрозам громадській безпеці, тому на опрацювання персональних даних для таких інших цілей у частині, що стосується сфери застосування законодавства Союзу, поширюється чинність цього Регламенту.

У сфері опрацювання персональних даних такими компетентними органами для цілей, на які поширюється сфера застосування цього Регламенту, державам-членам необхідно дозволити мати або запроваджувати більш уточнені положення для адаптації застосування норм цього Регламенту. Такими положеннями можна більш чітко визначити спеціальні вимоги до опрацювання персональних даних такими компетентними органами для зазначених інших цілей з огляду на конституційну, організаційну та адміністративну структуру відповідної держави-члени. Якщо на опрацювання персональних даних приватними органами поширюється сфера застосування цього Регламенту, у такому разі цей Регламент повинен надавати державам-членам можливість за особливих обставин вводити обмеження на законодавчому рівні щодо деяких обов'язків і прав у разі, якщо таке обмеження є необхідним і пропорційним заходом для захисту особливих важливих інтересів в демократичному суспільстві, зокрема для громадської безпеки та запобігання, виявлення чи переслідування за скоєння кримінальних злочинів або виконання кримінальних покарань,

---

* Директива Європейського Парламенту і Ради (ЄС) 2016/680 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування за вчинення кримінальних злочинів або виконання кримінальних покарань і про вільний рух таких даних, а також скасування Рамкового рішення Ради 2008/977/ЈНА (див. с. 89 цього Офіційного вісника).

у тому числі захисту від або запобігання загрозам громадській безпеці. Це доцільно, наприклад, у контексті боротьби з відмиванням грошей або діяльності лабораторій судових експертиз.

20. Оскільки дія цього Регламенту поширюється, окрім іншого, на діяльність судів та інших судових органів, у законодавстві Союзу або держав-членів можна чітко визначити операції і процедури опрацювання, пов'язані з опрацюванням персональних даних судами та іншими судовими органами. Компетенція наглядових органів не повинна поширюватися на опрацювання персональних даних у ситуаціях, коли суди діють як судові органи, для збереження їх незалежності у ході виконання ними судових функцій, у тому числі в процесі вироблення й ухвалення рішень. Необхідно надати можливість покладання обов'язків з нагляду за операціями опрацювання таких даних на спеціальні органи в межах судової системи держави-члена, які повинні, зокрема, забезпечувати дотримання норм цього Регламенту, підвищувати інформованість представників судових органів про їхні обов'язки за цим Регламентом і розглядати скарги у зв'язку з операціями опрацювання таких даних.

21. Цим Регламентом дотримано застосування Директиви Європейського Парламенту і Ради 2000/31/ЄС*, зокрема норм ст. 12–15 зазначеної Директиви про відповідальність надавачів посередницьких послуг. Зазначену Директиву спрямовано на сприяння належному функціонуванню внутрішнього ринку шляхом забезпечення вільного руху надання послуг інформаційного суспільства між державами-членами.

22. Будь-яке опрацювання персональних даних у контексті діяльності осідку контролера або оператора в Союзі необхідно здійснювати відповідно до цього Регламенту, незалежно від того, чи відбувається власне опрацювання в межах Союзу. Ефективна і реальна діяльність осідку передбачає стабільну організацію. У контексті згаданого правова форма такої організації, чи то через відділення, чи то через філію зі статусом юридичної особи, не є у цьому зв'язку визначальним фактором.

23. Для того, щоб фізичних осіб не було позбавлено захисту, на який вони мають право за цим Регламентом, на опрацювання персональних даних суб'єктів даних, які перебувають у Союзі, контролером або оператором, що не мають осідку в Союзі, повинна поширюватися сфера застосування цього Регламенту, якщо діяльність з опрацювання стосується надання товарів або постачання послуг таким суб'єктам даних, незалежно від того, чи пов'язані вони з платежем. Для встановлення факту пропонування товарів або постачання послуг таким контролером або оператором суб'єктам даних, що перебувають у Союзі, необхідно переконатися у тому, чи є очевидним те, що контролер або оператор передбачає постачання послуг

* Директива Європейського Парламенту і Ради 2000/31/ЄС від 8 червня 2000 р. про деякі правові аспекти послуг інформаційного суспільства, зокрема електронної комерції, на внутрішньому ринку («Директива про електронну комерцію») (OB L 178, 17.07.2000, с. 1).

суб'єктам даних в одній або декількох державах – членах Союзу. Оскільки власне доступність у межах Союзу веб-сайту контролера, оператора або посередника, або електронної адреси чи іншої контактної інформації, або використання мови, що є загальновживаною в третій країні, де має осідок контролер, є недостатньою для встановлення такого наміру, такі фактори, як використання мови або валюти, що є загальноприйнятими в одній або декількох державах-членах, із можливістю замовити товари чи послуги тією іншою мовою, або згадування споживачів чи користувачів, що перебувають у Союзі, підтверджують те, що контролер передбачає надання товарів або постачання послуг суб'єктам даних у Союзі.

24. Опрацювання персональних даних суб'єктів даних, які перебувають у Союзі, контролером або оператором, що мають осідок поза межами Союзу, необхідно також здійснювати з урахуванням цього Регламенту в частині моніторингу поведінки таких суб'єктів даних тією мірою, якою їхня поведінка має місце в межах Союзу. Для того, щоб визначити, чи можна вважати діяльність з опрацювання такою, яку провадять з метою моніторингу поведінки суб'єктів даних, необхідно встановити, чи є фізичні особи об'єктами відстежування в Інтернеті, у тому числі, чи може мати місце подальше використання методик опрацювання персональних даних, що складаються з профайлінгу фізичної особи, зокрема для ухвалення рішення щодо неї або нього чи для проведення аналізу, або передбачення її або його особистих переваг, поведінки чи ставлення.

25. Якщо законодавство держави-члена застосовують в силу норм публічного міжнародного права, цей Регламент необхідно також застосовувати до контролера, що має осідок поза межами Союзу, зокрема при дипломатичній місії держави-члена чи консульській установі.

26. Принципи захисту даних необхідно застосовувати до будь-якої інформації про фізичну особу, яку ідентифіковано чи можна ідентифікувати. Персональні дані із використанням псевдоніма, який можна приписати фізичній особі після використання додаткової інформації, необхідно розглядати як інформацію про фізичну особу, яку можна ідентифікувати. Щоб встановити можливість ідентифікації фізичної особи, необхідно взяти до уваги всі способи, що будуть використані з високою імовірністю, такі як відокремлення, контролером або іншою особою для ідентифікації фізичної особи прямо чи опосередковано. Для встановлення достатньої ймовірності використання способів для ідентифікації фізичної особи необхідно врахувати всі об'єктивні фактори, такі як витрати та період часу, необхідні для ідентифікації, з огляду на технології, наявні станом на момент опрацювання, і технологічні розробки. Принципи захисту даних, відповідно, не можна застосовувати до анонімної інформації, зокрема інформації, що не стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати, або персональних даних, що стали анонімними у такий спосіб, що суб'єкта даних неможливо чи більше неможливо ідентифікувати. Отже, цей Регламент не стосується

опрацювання такої анонімної інформації, у тому числі для статистичних або дослідницьких цілей.

27. Цей Регламент не застосовують до персональних даних померлих осіб. Держави-члени можуть запроваджувати норми щодо опрацювання персональних даних померлих осіб.

28. Використання псевдонімів до персональних даних може зменшити ризики для відповідних суб'єктів даних і допомогти контролерам і операторам у виконанні своїх обов'язків із захисту даних. Пряме запровадження означення «використання псевдоніма» у цьому Регламенті не передбачає обмеження будь-яких інших заходів щодо захисту даних.

29. Для створення стимулів використання псевдоніма під час опрацювання персональних даних заходи щодо використання псевдоніма повинні, дозволяючи при цьому загальний аналіз, уможливлювати їх використання самим контролером, якщо такий контролер застосував технічно-організаційні інструменти, необхідні для забезпечення, у відповідній ситуації опрацювання, виконання цього Регламенту, а також якщо додаткову інформацію для приписування персональних даних певному суб'єкту даних зберігають окремо. Контролер, який опрацювує персональні дані, повинен зазначити уповноважених осіб з числа тих, що працюють з тим самим контролером.

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

31. Органи публічної влади, яким розкривають персональні дані відповідно до передбаченого законом зобов'язання щодо виконання ними посадових функцій, такі як податкові та митні органи, служби фінансових розслідувань, незалежні адміністративні органи або органи державного регулювання фінансового ринку, відповідальні за регулювання та нагляд за фондовими ринками, не можна розглядати як одержувачів, якщо їм надають персональні дані, необхідні для певного розслідування у загальних інтересах, відповідно до законодавства Союзу або держави-члена. Запити на розкриття, які надають органи публічної влади, повинні завжди бути оформлені в письмовій формі, вмотивовані та призначені для спеціального випадку; вони не повинні впливати на всю картотеку або спричиняти взаємозалежність картотек. Такі органи публічної влади повинні опрацьовувати персональні дані з дотриманням норм щодо захисту даних і цілей опрацювання.

32. Згоду на опрацювання персональних даних суб'єкт повинен надавати шляхом чіткого ствердження, тобто у формі вільно наданого, конкретного, поінформованого та однозначного свідчення, зокрема, у формі письмової заяви, наданої в тому числі електронними засобами, або у формі

усної заяви. Це може бути позначка у клітинці, поставлена під час відвідування веб-сайту в мережі Інтернет, обране технічне налаштування для послуг інформаційного суспільства або інша заява чи поведінка, що чітко вказують на те, що суб'єкт даних погоджується із запропонованим опрацюванням персональних даних. Мовчання, автоматичне проставляння позначок у клітинках або бездіяльність, відповідно, не означають надання згоди. Згода повинна поширюватися на всі види опрацювання даних, здійснюваних для однакової цілі або цілей. Якщо опрацювання передбачає досягнення множинних цілей, згода потрібна для кожної з них. Якщо згоду суб'єкта даних необхідно надати після електронного запиту, у такому разі запит повинен бути чітким, точним і не передбачати надмірно негативних наслідків використання послуги, для якої його надають.

33. Часто на момент збирання даних неможливо чітко визначити мету опрацювання персональних даних для цілей наукового дослідження, тому суб'єкти даних повинні мати дозвіл на обробку даних у деяких сферах наукових досліджень, якщо в них дотримано визнаних етичних норм для наукового дослідження. Суб'єкти даних повинні мати можливість надавати свою згоду лише стосовно окремих сфер дослідження або частини дослідницьких проектів в обсязі, виправданому поставленою метою.

34. Необхідно означити генетичні характеристики як персональні дані, що стосуються вроджених або набутих генетичних ознак фізичної особи та отримані в результаті аналізу біологічної проби, взятої у певної фізичної особи, зокрема хромосомного аналізу, аналізів дезоксирибонуклеїнової кислоти (ДНК) або рибонуклеїнової кислоти (РНК), чи аналізу іншого компонента, що уможливлює отримання аналогічної інформації.

35. Персональні дані стосовно стану здоров'я повинні містити всі дані, пов'язані зі станом здоров'я суб'єкта даних, і розкривати інформацію про минулий, поточний або майбутній стан фізичного або психічного здоров'я суб'єкта даних. Це включає інформацію про фізичну особу, зібрану під час реєстрації на надання послуг або надання послуг у сфері охорони здоров'я, як вказано у Директиві Європейського Парламенту і Ради 2011/24/ЄС*, такій фізичній особі; номер, символьний знак або опис, що приписують фізичній особі для того, щоб однозначно ідентифікувати фізичну особу для цілей охорони здоров'я; інформацію, отриману внаслідок дослідження або огляду частини тіла чи речовини, що міститься в тілі, у тому числі з генетичних даних або біологічних проб; а також будь-яку інформацію, наприклад, про захворювання, недієздатність, ризик захворювання, історію хвороби, клінічне лікування або фізіологічний чи біомедичний стан здоров'я суб'єкта даних, незалежно від джерела її надходження, наприклад, від лікаря чи іншого медичного працівника, від лікарні, медичного обладнання або тестів лабораторної діагностики.

---

* Директива Європейського Парламенту і Ради 2011/24/ЄС від 9 березня 2011 р. про забезпечення прав пацієнтів на транскордонні послуги з охорони здоров'я (OB L 88, 4.04.2011, с. 45).

36. Головним осідком контролера в Союзі має бути місце розташування його центральної адміністрації в Союзі, за винятком прийняття рішень про цілі та засоби опрацювання в іншому осідку контролера в Союзі, у такому разі такий інший осідок необхідно вважати головним осідком. Головний осідок контролера в Союзі необхідно визначати за об'єктивними критеріями з огляду на результативну та фактичну управлінську діяльність, у ході якої ухвалюють ключові рішення щодо цілей і засобів опрацювання на основі стабільних домовленостей. Цей критерій не повинен залежати від того, чи опрацьовують персональні дані у такому місці. Наявність і використання технічних засобів і технологій опрацювання персональних даних або опрацювання даних не становлять як такі головний осідок та, відповідно, не є вирішальними критеріями для визначення головного осідку. Головним осідком оператора повинно бути місце розташування його центральної адміністрації у Союзі або, якщо його центральної адміністрації немає в Союзі, місце, де опрацьовують основні види даних у Союзі. У випадках залучення і контролера, і оператора компетентний головний наглядовий орган повинен залишатися наглядовим органом держави-члена, де має осідок контролер, але наглядовий орган оператора необхідно вважати відповідним наглядовим органом, і такий наглядовий орган повинен брати участь у процедурі співпраці, передбаченій цим Регламентом. У будь-якому разі наглядові органи держави-члена або держав-членів, у яких оператор має одне або декілька осідків, не можна вважати відповідними наглядовими органами, якщо проект рішення стосується лише контролера. Якщо опрацювання провадить група підприємств, головний осідок підприємства, що здійснює контроль, необхідно вважати головним осідком групи підприємств, за винятком випадку, коли цілі та засоби опрацювання визначено іншим підприємством.

37. Групу підприємств утворює підприємство, яке провадить контроль, і підприємства під його контролем, при цьому підприємство, яке провадить контроль, повинно бути підприємством, що має право здійснювати домінантний вплив на інші підприємства шляхом застосування, наприклад, права власності, фінансової участі чи правил, що її регулюють, або повноваження на застосування норм про опрацювання персональних даних. Підприємство, що контролює опрацювання персональних даних в афілійованих підприємствах, необхідно вважати разом з такими підприємствами групою підприємств.

38. Діти потребують особливого захисту в питанні персональних даних, оскільки вони можуть бути менш обізнаними про відповідні ризики, наслідки та гарантії, а також про свої права щодо опрацювання персональних даних. Такий особливий захист повинен, зокрема, застосовуватися до використання персональних даних дітей для цілей маркетингу або створення профілів особистості чи користувача, збирання персональних даних щодо дітей під час користування послугами, які пропонують безпосередньо дитині. Згоду особи, що несе батьківську відповідальність, не

можна вимагати в контексті надання профілактичних або консультаційних послуг безпосередньо дитині.

39. Будь-яке опрацювання персональних даних повинно бути законним і правомірним. Фізичні особи повинні бути обізнані про те, що їхні персональні дані збирають, використовують, обговорюють або іншим чином опрацьовують, а також про те, якою мірою опрацьовують чи опрацьовуватимуть персональні дані. Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення щодо опрацювання таких персональних даних були доступними і зрозумілими, з використанням чітких і простих формулювань. Цей принцип стосується, зокрема, інформування суб'єктів даних про особу контролера та цілі опрацювання і надання подальшої інформації для забезпечення правомірного і прозорого опрацювання в частині, що стосується відповідних фізичних осіб та їхнього права на отримання підтвердження та повідомлення про ті персональні дані, які їх стосуються та підлягають опрацюванню. Фізичні особи повинні бути обізнані про ризики, правила, гарантії та права щодо опрацювання персональних даних і про те, як реалізувати свої права у зв'язку з таким опрацюванням. Зокрема, спеціальні цілі опрацювання персональних даних повинні бути прямо вираженими і законними, а також означеними на момент збирання персональних даних. Персональні дані повинні бути достатніми, відповідними та обмежуватися тим, що необхідно для досягнення цілей, для яких їх опрацьовують. Це вимагає, зокрема, забезпечення того, що період, протягом якого зберігаються персональні дані, був скорочений до абсолютного мінімуму. Персональні дані необхідно опрацьовувати, лише якщо мети опрацювання не можна досягнути розумним чином іншими засобами. Щоб персональні дані не зберігалися довше, ніж це необхідно, контролер повинен установити часові межі для вилучення або періодичного перегляду. Необхідно вживати всіх відповідних заходів для забезпечення виправлення або вилучення неточних персональних даних. Персональні дані необхідно опрацьовувати в спосіб, що забезпечує відповідний рівень безпеки та конфіденційності персональних даних, у тому числі для запобігання несанкціонованому доступу або використанню персональних даних, а також обладнання, необхідного для опрацювання.

40. Щоб опрацювання було законним, персональні дані необхідно опрацьовувати на підставі згоди відповідного суб'єкта даних або на іншій законній підставі, передбаченій законом, або цим Регламентом, або іншим нормативно-правовим актом Союзу або держави-члена, як зазначено в цьому Регламенті, у тому числі за необхідності дотримання встановленого законом зобов'язання, яке поширюється на контролера, або за необхідності виконання договору, стороною якого є суб'єкт даних, або для вжиття заходів на запит суб'єкта даних перед укладенням договору.

41. Якщо цей Регламент містить покликання на законодавчу базу або законодавчий інструмент, ухвалення парламентом законодавчого акта, з дотриманням вимог, що відповідають конституційному порядку відповідної

держави-члена, є необов'язковим. Проте така законодавча база або такий законодавчий інструмент повинні бути чіткими і точними, а їх застосування повинно бути передбачуваним для осіб, яких вони стосуються, згідно з прецедентним правом Суду Європейського Союзу («Суд») і Європейського суду з прав людини.

42. У разі, якщо опрацювання здійснюють на підставі згоди суб'єкта даних, контролер повинен бути спроможним довести те, що суб'єкт даних надав згоду на операцію опрацювання. Зокрема, в контексті письмової заяви з іншого питання, гарантії повинні забезпечувати те, що суб'єкт даних обізнаний про факт і межі надання згоди. Згідно з Директивою Ради 93/13/ЄЕС*, заяву про надання згоди, попередньо сформульовану контролером, необхідно надавати в зрозумілій та доступній формі, з використанням чітких і простих формулювань, вона також не повинна містити неправомірні умови. Щоб згода вважалася поінформованою, суб'єкт даних повинен бути обізнаним, принаймні, про особу контролера та цілі опрацювання персональних даних. Згоду не можна вважати такою, що була добровільно надана, якщо суб'єкт даних не здійснює справжнього чи добровільного вибору або неспроможний відмовити в наданні згоди чи її відкликанні, не заподіюючи при цьому шкоди.

43. Щоб згода була визнана добровільною, вона не повинна передбачати необхідність застосування дійсних законних підстав опрацювання персональних даних у спеціальному випадку, коли існує помітний дисбаланс між суб'єктом даних і контролером, зокрема коли контролер є органом публічної влади і, тому, малоймовірно, що згоду було надано добровільно за усіх обставин такої спеціальної ситуації. Презумпція ненадання добровільної згоди виникає у разі, коли немає окремого дозволу на здійснення різних операцій опрацювання персональних даних, незважаючи на її відповідність окремому випадку, або якщо виконання договору, в тому числі, надання послуги, залежить від надання згоди, незважаючи на те, що така згода не є обов'язковою для такого виконання.

44. Опрацювання необхідно вважати законним у разі його необхідності для укладення договору або наміру щодо укладення договору.

45. Якщо опрацювання здійснюють відповідно до встановленого законом зобов'язання контролера, або якщо це необхідно для виконання завдання в суспільних інтересах або виконання офіційних повноважень, його необхідно провадити на підставі нормативно- правового акту Союзу чи держави-члена. Цей Регламент не вимагає ухвалення спеціального нормативно-правового акта для кожного окремого опрацювання. Нормативно-правового акта як підстави для здійснення декількох операцій з опрацювання, що ґрунтуються на виконанні встановленого законом зобов'язання контролера, або, за необхідності, виконанні завдання в суспільних інтересах чи здійсненні офіційних повноважень, може бути достатньо. Ціль опрацювання повинен

* Директива Ради 93/13/ЄЕС від 5 квітня 1993 р. про несправедливі умови споживчих договорів (OB L 95, 21.04.1993, с. 29).

встановлювати безпосередньо нормативно-правовий акт Союзу або держави-члена. Крім того, такий нормативно-правовий акт може визначати загальні умови цього Регламенту, що регулюють законність опрацювання персональних даних, встановлювати технічні вимоги до визначення контролера, тип персональних даних, що підлягають опрацюванню, відповідних суб'єктів даних, установи, яким дозволено розкривати персональні дані, цільові обмеження, період зберігання та інші заходи для забезпечення законного та правомірного опрацювання. Також саме нормативно-правовий акт Союзу або держави-члена визначає, чи повинен контролер, який виконує завдання в суспільних інтересах або для здійснення офіційних повноважень, бути органом публічної влади або ще однією фізичною або юридичною особою, діяльність якої регулюється публічним правом, або, якщо це зумовлено суспільними інтересами, у тому числі для таких цілей, як охорона суспільного здоров'я та соціальний захист і управління послугами в сфері охорони здоров'я, приватним правом, зокрема професійною асоціацією.

46. Опрацювання персональних даних необхідно також вважати законним, якщо постає необхідність захистити інтерес, важливий для життя суб'єкта даних або життя ще однієї фізичної особи. Опрацювання персональних даних на підставі життєво важливого інтересу іншої фізичної особи повинно мати місце лише у випадку, коли опрацювання неможливо відкрито здійснювати на іншій законній підставі. Деякі типи опрацювання можуть ґрунтуватися на важливих підставах суспільного інтересу та життєво важливих інтересів суб'єкта даних, наприклад, якщо опрацювання є необхідним для гуманітарних цілей, у тому числі моніторингу епідемій та їх розповсюдження, чи за надзвичайних гуманітарних ситуацій, зокрема в ситуаціях стихійних лих і антропогенних катастроф.

47. Законні інтереси контролера, в тому числі інтереси, задля яких можна розкрити персональні дані, або законні інтереси третьої сторони можуть передбачати необхідність законодавчої бази опрацювання за умови, що інтереси чи фундаментальні права або свободи суб'єкта даних не є пріоритетними, враховуючи розумні очікування суб'єктів даних, засновані на їхніх відносинах з контролером. Такий законний інтерес може існувати, якщо існують відповідні та належні відносини між суб'єктом даних і контролером у ситуаціях, наприклад, коли суб'єкт даних є клієнтом або перебуває на службі в контролера. У будь-якому разі існування законного інтересу потребуватиме ретельного оцінювання, а саме, чи може суб'єкт даних відповідним чином очікувати ймовірного проведення опрацювання для такої цілі на момент збирання і в контексті збирання персональних даних. Інтереси та фундаментальні права суб'єкта даних можуть, зокрема, переважати над інтересами контролера даних, якщо опрацювання персональних даних відбувається за обставин, коли суб'єкти даних відповідним чином не очікують подальшого опрацювання. З огляду на те, що саме законодавець повинен передбачити законодавчу базу для опрацювання

персональних даних органами публічної влади, таку законодавчу базу не можна застосовувати до опрацювання даних органами публічної влади під час виконання своїх функцій. Опрацювання персональних даних винятково для цілей запобігання шахрайству також становить законний інтерес відповідного контролера даних. Опрацювання персональних даних для цілей прямого маркетингу можна вважати опрацюванням, що здійснюється для забезпечення законного інтересу.

48. Контролери, які є частиною групи підприємств чи установ, афілійованих з центральним органом, можуть мати законний інтерес у передаванні персональних даних усередині групи підприємств для внутрішніх адміністративних цілей, у тому числі для опрацювання персональних даних клієнтів або працівників. Загальні принципи передавання персональних даних, що діють всередині групи підприємств, до підприємства, розташованого в третій країні, залишаються без змін.

49. Опрацювання персональних даних мірою, що є надзвичайно необхідною та пропорційною цілям забезпечення мережевої та інформаційної безпеки, тобто здатності мережі чи інформаційної системи чинити опір, на певному рівні довіри, випадковим подіям або незаконним чи зловмисним діям, що ставлять під загрозу наявність, автентичність, цілісність і конфіденційність збережених або переданих персональних даних, і безпеки пов'язаних послуг, які пропонують через такі мережі чи системи або надають за їх допомогою доступ органи публічної влади, групи з реагування на надзвичайні ситуації в комп'ютерній сфері (CERT), групи для реагування на інциденти в сфері комп'ютерної безпеки (CSIRT), провайдери електронних мереж і послуг зв'язку та провайдери технологій і послуг у сфері безпеки, становить законний інтерес відповідного контролера даних. Це, наприклад, може включати запобігання несанкціонованому доступу до електронних мереж зв'язку і розподілу шкідливого коду, припинення атак на «відмову в обслуговуванні», а також пошкодження комп'ютера та систем електронного зв'язку.

50. Дозвіл на опрацювання персональних даних для інших цілей, на відміну від тих, для яких здійснювали первинне збирання персональних даних, необхідно надавати лише тоді, коли опрацювання сумісне із первинними цілями збирання персональних даних. У такому разі немає необхідності в будь-якій законодавчій базі, відокремленій від такої, якою вже дозволено збирання персональних даних. Якщо опрацювання персональних даних необхідне для виконання завдання в публічних інтересах або виконання офіційних повноважень, покладених на контролера, законодавство Союзу або держави-члена може визначити та уточнити завдання і цілі, для виконання яких необхідно вважати сумісним і законним подальше опрацювання. Подальше опрацювання для архівних цілей у публічних інтересах, цілей наукового або історичного дослідження, статистичних цілей необхідно вважати сумісним із законними операціями опрацювання. Законодавча база, передбачена законодавством Союзу або держави-члени

щодо опрацювання персональних даних, може слугувати законодавчою базою для подальшого опрацювання. Для встановлення сумісності цілей подальшого опрацювання і первинного збирання персональних даних контролер, виконавши всі вимоги щодо законності первинного опрацювання, повинен враховувати, між іншим: будь-який зв'язок між тими цілями та цілями запланованого подальшого опрацювання; контекст, у якому збирають персональні дані, зокрема розумні очікування суб'єктів даних, засновані на їхніх домовленостях з контролером щодо їх подальшого використання; специфіку персональних даних; наслідки запланованого подальшого опрацювання для суб'єктів даних; існування належних гарантій, як у первинній, так і в подальшій операціях опрацювання.

Якщо суб'єкт даних надав згоду, або якщо опрацювання здійснюють на основі законодавства Союзу чи держави-члена, що становить необхідний і пропорційний інструмент демократичного суспільства для охорони, зокрема, важливих цілей загального суспільного інтересу, контролер повинен отримати дозвіл на подальше опрацювання персональних даних, незалежно від сумісності цілей. У будь-якому разі необхідно забезпечити застосування принципів, встановлених цим Регламентом, та, зокрема, інформування суб'єкта даних про такі інші цілі та про його або її права, у тому числі про право на заперечення. Повідомлення контролера про можливі кримінальні діяння або загрози громадській безпеці, а також передавання компетентному органу відповідних персональних даних в окремих випадках або в декількох ситуаціях, що стосуються такого самого кримінального діяння або загроз громадській безпеці, необхідно вважати такими, що відповідають законному інтересу контролера. Проте таке передавання, що відповідає законному інтересу контролера, або подальше опрацювання персональних даних необхідно заборонити, якщо опрацювання є несумісним із встановленими законом, професійними або іншими обов'язковими до виконання зобов'язаннями щодо збереження таємниці.

51. Персональні дані, що, за своєю специфікою, є особливо чутливими щодо фундаментальних прав і свобод, потребують особливого захисту, оскільки контекст їх опрацювання може створити істотні ризики для фундаментальних прав і свобод. Такі персональні дані повинні включати персональні дані, що розкривають расову або етнічну приналежність, а відтак використання терміна «расова приналежність» у цьому Регламенті не передбачає прийняття Союзом теорій, що намагаються визначити існування окремих людських рас. Опрацювання фотографій не можна систематично вважати опрацюванням спеціальних категорій персональних даних, оскільки термін «біометричні дані» на них поширюється, лише якщо їх опрацьовують за допомогою спеціальних технічних засобів, що дають змогу однозначно ідентифікувати або аутентифікувати фізичну особу. Такі персональні дані не можна опрацьовувати, за винятком, якщо це дозволено в спеціальних випадках, визначених у цьому Регламенті, враховуючи, що законодавство держави-члени може містити спеціальні положення щодо

захисту даних для того, щоб адаптувати застосування норм цього Регламенту з метою дотримання встановленого законом зобов'язання, виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера. Додатково до спеціальних вимог щодо такого опрацювання необхідно застосовувати загальні принципи і норми цього Регламенту, зокрема в частині умов щодо правомірного опрацювання. Необхідно чітко окреслити відступи із загальної заборони на опрацювання таких спеціальних категорій персональних даних, зокрема, якщо суб'єкт даних надає свою чітку згоду або в разі виникнення особливих потреб, наприклад, коли опрацювання здійснюють у ході реалізації законних видів діяльності окремими асоціаціями або фондами, ціль якої полягає у тому, щоб дозволити реалізацію фундаментальних свобод.

52. Також необхідно дозволити відступи із від заборони на опрацювання спеціальних категорій персональних даних, якщо це передбачено нормативно-правовим актом Союзу або держави-члена та згідно з відповідними гарантіями, для того, щоб захистити персональні дані та інші фундаментальні права, якщо це відповідає суспільному інтересу, а саме опрацювання персональних даних у галузі трудового законодавства, законодавства про соціальний захист, у тому числі про пенсійне забезпечення та забезпечення безпеки в галузі охорони здоров'я, цілей моніторингу та попередження, запобігання або контролю за інфекційними захворюваннями та іншими серйозними загрозами для здоров'я. Такий відступ можна зробити для цілей охорони здоров'я, у тому числі охорони суспільного здоров'я та управління послугами в сфері охорони здоров'я, особливо для того, щоб забезпечити якість та економію витрат на процедури врегулювання претензій стосовно пільг і послуг у системі медичного страхування або для досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження, статистичних цілей. Також відступ повинен дозволяти опрацювання таких персональних даних, якщо це необхідно для формування, здійснення або захисту правових претензій, під час судового провадження або в межах адміністративної чи позасудової процедури.

53. Опрацювання спеціальних категорій персональних даних, що потребують вищого ступеня захисту, дозволено здійснювати для цілей, пов'язаних з охороною здоров'я, лише якщо необхідно досягнути таких цілей в інтересах фізичних осіб та усього суспільства, зокрема в контексті управління послугами та системами з охорони здоров'я та соціального забезпечення, у тому числі опрацювання таких даних органами з управління та центральними органами з охорони здоров'я для цілей проведення контролю якості, управління інформацією та загального національного і місцевого нагляду за системою охорони здоров'я чи соціального забезпечення, а також забезпечення безперервності охорони здоров'я чи соціального забезпечення та транскордонної охорони здоров'я або безпеки в сфері охорони здоров'я, цілей моніторингу та попередження чи для досягнення цілей в інтересах суспільства, цілей наукового чи історичного дослідження,

статистичних цілей, на підставі законодавства Союзу чи держави-члена, що має відповідати суспільним інтересам, а також для навчання, яке проводять в інтересах суспільства в сфері охорони суспільного здоров'я. Тому цей Регламент повинен передбачати гармонізовані умови опрацювання спеціальних категорій персональних даних стосовно стану здоров'я, з урахуванням особливих потреб, зокрема, якщо такі дані опрацьовують особи, на яких законом покладено зобов'язання щодо збереження професійної таємниці, для певних цілей, пов'язаних із здоров'ям. Законодавство Союзу чи держави-члена повинно передбачати спеціальні та належні гарантії для захисту фундаментальних прав і персональних даних фізичних осіб. Державам-членам необхідно дозволити мати або запроваджувати умови, в тому числі обмеження, у зв'язку з опрацюванням генетичних даних, біометричних даних або даних стосовно стану здоров'я. Проте це не повинно перешкоджати вільному переміщенню персональних даних у межах Союзу тоді, коли такі умови застосовують до транскордонного опрацювання таких даних.

54. Опрацювання спеціальних категорій персональних даних може бути необхідним у цілях задоволення суспільних інтересів у сфері охорони суспільного здоров'я без згоди суб'єкта даних. На таке опрацювання поширюється застосування відповідних і спеціальних інструментів для захисту прав і свобод фізичних осіб. У такому контексті «суспільне здоров'я» необхідно тлумачити так, як це означено в Регламенті Європейського Парламенту і Ради (ЄС) № 1338/2008*, зокрема, як усі елементи, що стосуються здоров'я, а саме стан здоров'я, у тому числі захворюваність і недієздатність, визначальні чинники, що впливають на стан здоров'я, потребу в послугах з охорони здоров'я, надання та універсальний доступ до охорони здоров'я, витрати на послуги з охорони здоров'я та їх фінансування, причини смертності. Таке опрацювання даних стосовно стану здоров'я для цілей суспільних інтересів не повинно призводити до опрацювання персональних даних для інших цілей третіми сторонами, такими як працедавці або страхові компанії чи банківські установи.

55. Крім того, опрацювання персональних даних офіційними органами для досягнення цілей, встановлених конституційним правом або міжнародним публічним правом, офіційно визнаних релігійних об'єднань необхідно здійснювати з урахуванням суспільного інтересу.

56. У ході виборчого процесу функціонування демократичної системи в державі-члені вимагає збирання політичними партіями персональних даних про політичні переконання населення. Дозвіл на опрацювання таких даних можна надавати з урахуванням суспільного інтересу, за умови впровадження відповідних заходів безпеки.

---

* Регламент Європейського Парламенту і Ради (ЄС) № 1338/2008 від 16 грудня 2008 р. про статистику Співтовариства з охорони суспільного здоров'я, охорони здоров'я та безпеки на робочому місці (OB L 354, 31.12.2008, с. 70).

57. Якщо персональні дані, які опрацьовує контролер, не надають йому можливості ідентифікувати фізичну особу, контролер даних не повинен бути зобов'язаним отримувати додаткову інформацію для того, щоб ідентифікувати суб'єкта даних винятково для цілей дотримання будь-якого положення цього Регламенту. Проте контролер не повинен відмовлятися від додаткової інформації, яку надає суб'єкт даних для підтримки реалізації своїх прав. Ідентифікація повинна включати цифрову ідентифікацію суб'єкта даних, наприклад, за допомогою механізму аутентифікації, такого як однакові облікові дані, які використовує суб'єкт даних для того, щоб увійти в онлайн-сервіс, запропонований контролером даних.

58. Принцип прозорості вимагає, щоб будь-яка інформація, призначена для громадськості або суб'єкта даних, була стислою і зрозумілою, чітко і просто сформульованою, а також, за необхідності, із застосуванням засобів візуалізації. Таку інформацію можна надавати в електронному форматі, наприклад, через веб-сайт, коли її адресовано громадськості. Це, зокрема, доцільно у ситуаціях, коли збільшення кількості агентів і технологічна складність практичної діяльності перешкоджають обізнаності та розумінню суб'єктом даних того, чи збирають її або його персональні дані, хто їх збирає і для якої цілі, як, наприклад, у випадку онлайн-реклами. З огляду на те, що діти потребують особливого захисту, будь-яку інформацію та повідомлення, у випадку, якщо опрацювання призначено для дитини, необхідно формулювати чітко і просто, щоб дитина могла легко зрозуміти.

59. Необхідно забезпечити умови для сприяння реалізації прав суб'єктів даних відповідно до цього Регламенту, в тому числі механізми надання запиту та, за необхідності, отримання, на безоплатній основі, зокрема, доступу до персональних даних, можливості їх виправлення та вилучення, а також реалізації права на заперечення. Контролер повинен також надати засоби для уможливлення подання запитів у електронному форматі, особливо, якщо персональні дані опрацьовують електронними засобами. Контролер повинен бути зобов'язаним відповідати на запити суб'єкта даних без необґрунтованої затримки та щонайменше протягом одного місяця, а також зазначати причини, якщо контролер не має наміру виконувати будь-який такий запит.

60. Принципи правомірного та прозорого опрацювання вимагають, щоб суб'єкта даних було поінформовано про операцію опрацювання та її цілі. Контролер повинен надавати суб'єкту даних будь-яку подальшу інформацію, необхідну для забезпечення правомірного та прозорого опрацювання, враховуючи конкретні обставини та контекст, що супроводжують опрацювання персональних даних. Крім того, необхідно поінформувати суб'єкта даних про наявність профайлінгу та наслідки такого профайлінгу. У разі отримання персональних даних від суб'єкта даних, його або її також необхідно поінформувати про те, чи зобов'язаний він або вона надати персональні дані, та про наслідки ненадання таких даних. Таку інформацію можна надавати в поєднанні зі стандартизованими іконками для того,

щоб наочно, доступним для розуміння та чітким способом розкрити зміст запланованого опрацювання. Представлені в електронному форматі іконки повинні легко зчитуватися машиною.

61. Інформацію щодо опрацювання персональних даних про суб'єкта даних необхідно надавати йому або їй у момент отримання даних від суб'єкта даних або, якщо персональні дані отримано з іншого джерела, в розумний строк, залежно від обставин конкретної ситуації. Якщо персональні дані можна законним шляхом розкрити ще одному одержувачу, суб'єкта даних необхідно поінформувати про це під час первинного розкриття персональних даних одержувачу. Якщо контролер має намір опрацьовувати персональні дані для цілі, іншої ніж та, для якої їх збирали, контролер повинен надати суб'єкту даних, до моменту подальшого опрацювання, інформацію про таку іншу ціль та іншу необхідну інформацію. Якщо суб'єкту даних неможливо надати інформацію про походження персональних даних, оскільки були використані різні джерела, у такому разі необхідно надати загальну інформацію.

62. Проте немає необхідності вимагати надання такої інформації, якщо суб'єкт даних уже володіє інформацією, якщо процедури реєстрації та розкриття персональних даних чітко регламентовані в нормативно-правовому акті або якщо надання інформації суб'єкту даних виявляється неможливим чи може викликати непропорційні наслідки. Остання ситуація може, зокрема, мати місце, якщо опрацювання здійснюють для задоволення суспільних інтересів, цілей наукового чи історичного дослідження, статистичних цілей. За таких обставин необхідно враховувати кількість суб'єктів даних, тривалість існування даних і будь-які відповідні запобіжні заходи, яких було вжито.

63. Суб'єкт даних повинен мати право доступу до персональних даних, які збирають щодо нього, і реалізовувати таке право вільно та через розумні проміжки часу для того, щоб бути обізнаним про законність опрацювання та перевірити її. Це включає право суб'єктів даних мати доступ до інформації, що стосується їхнього здоров'я, наприклад у медичних документах, що містять таку інформацію, як діагнози, результати обстеження, оцінювань, які проводять лікарі-куратори, і будь-які інше надане лікування або втручання. Кожен суб'єкт даних повинен, таким чином, мати право знати й отримувати інформацію, зокрема про цілі, для яких опрацьовують персональні дані; за можливості, про період, протягом якого опрацьовують персональні дані; одержувачів персональних даних; логіку, що зумовлює будь-яке автоматизоване опрацювання персональних даних, і принаймні, що базується на профайлінгу; наслідки такого опрацювання. За можливості, контролер повинен бути спроможним надавати віддалений доступ до системи безпеки, яка б забезпечила суб'єкту даних прямий доступ до своїх персональних даних. Таке право не повинно негативно впливати на права чи свободи інших осіб, у тому числі комерційні таємниці чи інтелектуальну власність та, зокрема, авторське право в галузі захисту програмного

забезпечення. Проте наслідком таких обговорень не повинна бути відмова надати усю інформацію суб'єкту даних. Якщо контролер опрацьовує великі обсяги інформації про суб'єкта даних, він повинен мати можливість надіслати запит про те, щоб до моменту надсилання інформації суб'єкт даних вказав інформацію або види опрацювання даних, яких стосується запит.

64. Контролер повинен вживати усіх відповідних заходів для перевірки особи суб'єкта даних, який надсилає запит на отримання доступу, зокрема в контексті онлайн-сервісів та онлайн-ідентифікаторів. Контролер не повинен утримувати персональні дані лише з метою мати можливість відреагувати на потенційні запити.

65. Суб'єкт даних повинен мати право на виправлення своїх персональних даних і «право бути забутим», якщо утримання таких даних порушує цей Регламент або законодавство Союзу чи держави-члени, яке поширюється на контролера. Зокрема, суб'єкт даних повинен мати право на вилучення своїх персональних даних і припинення їх опрацювання, якщо персональні дані більше не потрібні для цілей, для яких їх збирають або іншим чином опрацьовують, якщо суб'єкт даних відкликав свою згоду або заперечує проти опрацювання його або її персональних даних, або якщо опрацювання його чи її персональних даних іншим чином не відповідає цьому Регламенту. Таке право є доцільним, зокрема, коли суб'єкт даних надав свою згоду, будучи дитиною, та не є повністю обізнаним про ризики, пов'язані з опрацюванням, а пізніше хоче вилучити такі персональні дані, особливо з мережі Інтернет. Суб'єкт даних повинен мати можливість реалізувати таке право, незважаючи на те, що він більше не є дитиною. Проте подальше утримання персональних даних повинно бути законним, за необхідності, для реалізації права на свободу вияву поглядів і свободу інформації, дотримання встановленого законом зобов'язання, виконання завдання, зумовленого суспільними інтересами чи офіційними повноваженнями, покладеними на контролера, суспільними інтересами в сфері охорони суспільного здоров'я, цілями наукового чи історичного дослідження, статистичними цілями, або для формування, здійснення чи захисту законного права вимоги.

66. Для посилення права бути забутим в електронному середовищі необхідно також розширити право на вилучення таким чином, щоб контролер, який оприлюднив персональні дані, був зобов'язаний поінформувати контролерів, які опрацьовують такі персональні дані, вилучити будь-які посилання на такі персональні дані або їх копії чи відтворення. Для цього контролер повинен вживати відповідних заходів з використанням доступних йому технологій та інструментів.

67. Методи обмеження опрацювання персональних даних можуть включати, серед іншого, тимчасове перенесення обраних даних до іншої системи опрацювання, що робить їх недоступними для користувачів, або тимчасове вилучення опублікованих даних зі сторінки в мережі Інтернет. В автоматизованих картотеках обмеження опрацювання необхідно забез-

печувати технічними інструментами у спосіб, що унеможливлює подальше опрацювання і внесення змін до персональних даних. Необхідно чітко вказувати в системі, що опрацювання персональних даних є обмеженим.

68. Для посилення контролю за власними даними, які опрацьовують автоматизованими засобами, суб'єкт даних повинен мати право на отримання своїх персональних даних, які він надав контролеру в структурованому, широко вживаному форматі, що легко зчитується машиною, і на передавання їх іншому контролеру. Необхідно заохочувати контролерів даних розробляти сумісні формати, щоб уможливити мобільність даних. Таке право необхідно застосовувати, якщо суб'єкт даних надав персональні дані на підставі своєї згоди або якщо опрацювання є необхідним для виконання договору. Його не можна застосовувати, якщо опрацювання ґрунтується на законній підставі, іншій ніж згода чи договір. Таке право не можна реалізовувати стосовно контролерів, які опрацьовують персональні дані під час виконання своїх службових обов'язків. Його не можна застосовувати, якщо опрацювання персональних даних є необхідним для дотримання встановленого законом зобов'язання контролера, для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера. Право суб'єкта даних передавати або одержувати свої персональні дані не повинно створювати для контролерів обов'язок розробити або зберегти технічно сумісні системи опрацювання. У разі залучення декількох суб'єктів даних, в певному наборі персональних даних, право одержати персональні дані не повинно обмежувати права та свободи інших суб'єктів даних, згідно з цим Регламентом. Крім того, таке право не повинно обмежувати право суб'єкта даних на вилучення персональних даних і обмеження такого права, як передбачено цим Регламентом, не повинно, зокрема, передбачати вилучення персональних даних суб'єкта даних, які були надані ним або нею для виконання договору мірою та протягом періоду необхідності персональних даних для виконання договору. В разі необхідності суб'єкт даних повинен мати право на те, щоб персональні дані були передані безпосередньо від одного контролера до іншого.

69. Якщо персональні дані можна опрацьовувати на законних підставах, оскільки опрацювання обґрунтоване суспільними інтересами чи виконанням офіційних повноважень, покладених на контролера, або зумовлене законними інтересами контролера чи третьої сторони, суб'єкт даних повинен, тим не менше, мати право на заперечення проти опрацювання будь-яких персональних даних, що стосуються його або її конкретної ситуації. Обов'язком контролера є довести, що його законний інтерес переважає над інтересами або фундаментальними правами та свободами суб'єкта даних.

70. У разі опрацювання персональних даних для цілей прямого маркетингу суб'єкт даних повинен мати право на заперечення проти такого опрацювання, у тому числі профайлінгу, тією мірою, якою це стосується такого прямого маркетингу, у зв'язку з первинним чи подальшим опрацюванням, у будь-який час і на безоплатній основі. Інформацію про таке

право необхідно однозначно довести до відома суб'єкта даних і подати чітко та відокремлено від будь-якої іншої інформації.

71. Суб'єкт даних повинен мати право не виконувати рішення, що може передбачати вжиття заходу з оцінювання його або її персональних аспектів, винятково на підставі автоматизованого опрацювання, та яке породжує правові наслідки для нього чи неї або подібним чином істотно впливає на нього чи неї, а саме, автоматичну відмову в онлайн-заявці на кредит або практику наймання працівників за допомогою Інтернет-ресурсів без будь-якого втручання людини. Таке опрацювання включає «профайлінг», що складається з будь-якої форми автоматизованого опрацювання персональних даних із оцінюванням персональних аспектів, що стосуються фізичної особи, зокрема для аналізу або передбачення аспектів, що стосуються продуктивності суб'єкта даних на роботі, економічної ситуації, здоров'я, особистих переваг або інтересів, надійності або поведінки, місцезнаходження або пересування, якщо воно породжує правові наслідки, що стосуються його чи її, чи подібним чином істотно впливає на нього чи неї. Проте дозвіл на вироблення й ухвалення рішень на підставі такого опрацювання, в тому числі профайлінгу, необхідно надавати в разі, якщо це чітко передбачено законодавством Союзу чи держави-члена, яке поширюється на контролера, у тому числі для цілей моніторингу, запобігання шахрайству та ухиленню від сплати податків, що здійснюють відповідно до регламентів, стандартів і рекомендацій установ Союзу чи національних органів з нагляду і для гарантування безпеки і надійності послуги, яку постачає контролер, або необхідних для укладення чи виконання договору між суб'єктом даних і контролером, або якщо суб'єкт даних надав свою чітку згоду. У будь-якому разі таке опрацювання необхідно здійснювати згідно з відповідними гарантіями, що повинні передбачати надання конкретної інформації суб'єкту даних і право на втручання людини, висловлення своєї думки, отримання обґрунтування рішення, досягнутого після такого оцінювання, і оскарження рішення. Такий захід не повинен стосуватися дітей.

Щоб забезпечити правомірне та прозоре опрацювання інформації, що стосується суб'єкта даних, враховуючи конкретні обставини та контекст, у якому опрацьовують персональні дані, контролер повинен застосувати відповідні математичні або статистичні процедури для профайлінгу, вжити необхідних технічних і організаційних заходів, необхідних для гарантування, зокрема, того, що фактори, які спричиняють неточності в персональних даних, виправлено, а ризик помилок скорочено, охороняти персональні дані в спосіб, що враховує потенційні ризики для інтересів і прав суб'єкта даних і запобігає, серед іншого, дискримінаційним наслідкам для фізичних осіб на підставі расової чи етнічної приналежності, політичних переконань, релігії або вірувань, членства в професійних союзах, генетичного стану або стану здоров'я, чи сексуальної орієнтації, або того, що спричиняє вжиття заходів із такими наслідками. Дозвіл на автоматизоване вироблення й

ухвалення рішень і профайлінг на підставі спеціальних категорій персональних даних необхідно надавати лише за спеціальних умов.

72. Профайлінг регулюють такі норми цього Регламенту щодо опрацювання персональних даних, як законодавчі підстави принципів опрацювання або захисту даних. Необхідно уповноважити Європейську раду із захисту даних, засновану цим Регламентом («Рада»), надавати настанови у таких питаннях.

73. Обмеження щодо спеціальних принципів і прав на інформацію, доступ до персональних даних, їх виправлення або вилучення, права на мобільність даних, права на заперечення, рішень, що засновані на профайлінгу, а також повідомлення суб'єкта даних про порушення захисту персональних даних і інших пов'язаних зобов'язань контролерів можна запроваджувати в законодавство Союзу або держави-члена, наскільки це необхідно та доцільно в демократичному суспільстві для гарантування громадської безпеки, в тому числі для захисту життя людини, зокрема за умов стихійного лиха й антропогенних катастроф, запобігання, розслідування і переслідування осіб за скоєння кримінальних злочинів або виконання кримінальних покарань, у тому числі захисту від загроз громадській безпеці та запобігання їм, або за порушення етичних норм для регульованих професій, для захисту інших суспільних інтересів Союзу або держави-члена, зокрема важливих економічних або фінансових інтересів Союзу або держави-члена, ведення публічних реєстрів на підставі загального суспільного інтересу, подальшого опрацювання архівних персональних даних для надання конкретної інформації, що стосується політичної поведінки під колишніми тоталітарними державними режимами, або захисту суб'єктів даних, прав і свобод інших людей, у тому числі соціального захисту, цілей охорони здоров'я населення або гуманітарних цілей. Зазначені обмеження повинні відповідати вимогам, викладеним у Хартії та Європейській конвенції про захист прав людини та фундаментальних свобод.

74. Необхідно визначити обов'язки та відповідальність контролера щодо будь-якого опрацювання персональних даних, яке здійснює контролер або яке здійснюють від імені контролера. Зокрема, контролер повинен бути зобов'язаним забезпечити вжиття необхідних і результативних заходів і бути спроможним довести відповідність діяльності з опрацювання даних цьому Регламенту, в тому числі дієвість заходів. Такі заходи повинні враховувати специфіку, масштаби, контекст і цілі опрацювання та ризик для прав і свобод фізичних осіб.

75. Ризик для прав і свобод фізичних осіб, різної ймовірності та тяжкості, може стати результатом опрацювання персональних даних, що може призвести до фізичної, матеріальної та нематеріальної шкоди, зокрема: коли опрацювання може спричинити дискримінацію, крадіжку персональних даних або шахрайство, фінансові втрати, шкоду репутації, втрату конфіденційності персональних даних, які захищають як особисту таємницю, несанкціоноване скасування використання псевдонімів або будь-яку іншу

істотну економічну або соціальну шкоду; коли суб'єкти даних можуть бути позбавлені своїх прав і свобод або можливості контролю над своїми персональними даними; коли опрацьовують персональні дані, що розкривають расову або етнічну приналежність, політичні переконання, релігію або філософські переконання, членство в професійних союзах, і опрацьовують генетичні дані, дані про стан здоров'я або про сексуальне життя, про судимості та кримінальні злочини або пов'язані заходи безпеки; коли оцінюють персональні аспекти, зокрема з аналізом або передбаченням аспектів, що стосуються продуктивності праці, економічної ситуації, здоров'я, особистих переваг або інтересів, надійності або поведінки, місцезнаходження або пересування, для створення або використання особистих профілів; коли опрацьовують персональні дані вразливих категорій фізичних осіб, зокрема дітей; або коли опрацювання передбачає використання великих обсягів персональних даних і впливає на велику кількість суб'єктів даних.

76. Потрібно визначати ймовірність і тяжкість ризику для прав і свобод суб'єкта даних, спираючись на специфіку, масштаб, контекст і цілі опрацювання. Ризик необхідно визначати на основі об'єктивної оцінки, на підставі якої встановлюють, чи містять операції опрацювання даних ризик або високий ризик.

77. Рекомендації щодо реалізації відповідних заходів і доведення їх доцільності контролером або оператором, зокрема, стосовно визначення ризику, пов'язаного з опрацюванням, його оцінюванням у контексті походження, специфіки, ймовірності та тяжкості, визначенням прикладів кращої практики для зниження ризику, можна надати, зокрема, послуговуючись узгодженими кодексами поведінки, затвердженими сертифікатами, настановами, наданими Радою, або рекомендаціями співробітників з питань захисту даних. Рада може також видавати настанови щодо операцій опрацювання, які розглядаються як операції, що малоймовірно пов'язані з високим ризиком для прав і свобод фізичних осіб, і зазначати заходи, які можуть бути достатніми в таких ситуаціях для зниження ризиків.

78. Захист прав і свобод фізичних осіб у зв'язку з опрацюванням персональних даних вимагає застосування відповідних технічних та організаційних інструментів для забезпечення виконання вимог цього Регламенту. Щоб мати можливість підтвердити відповідність цьому Регламенту, контролер повинен ухвалити норми внутрішньої політики та забезпечити застосування інструментів, що відповідають, зокрема, принципам захисту даних за призначенням і захисту даних за замовчуванням. Такі заходи можуть передбачати, серед іншого, скорочення опрацювання персональних даних, якомога швидше використання псевдонімів, прозорість опрацювання персональних даних, надання суб'єктові даних можливості відстежувати опрацювання даних, а контролерові створювати та вдосконалювати характеристики безпеки. Під час створення, розроблення, добору та використання застосунків, сервісів і продуктів, що засновані на опрацюванні персональних даних або при опрацюванні персональних даних для виконання своїх

завдань, необхідно заохочувати виробників продуктів, сервісів і застосунків враховувати право на захист даних під час створення та розроблення таких продуктів, сервісів і застосунків і, за належного дотримання сучасного рівня розвитку, переконуватися, що контролери й оператори здатні виконувати свої зобов'язання щодо захисту даних. Принципи захисту даних за призначенням і захисту даних за замовчуванням необхідно також враховувати в контексті публічних тендерів.

79. Захист прав і свобод суб'єктів даних, а також обов'язки та відповідальність контролерів і операторів, пов'язані з моніторингом наглядових органів і здійснювані за допомогою їхніх засобів, вимагають чіткого розподілу обов'язків за цим Регламентом, у тому числі тоді, коли контролер визначає цілі та засоби опрацювання спільно з іншими контролерами або коли операцію з опрацювання здійснюють від імені контролера.

80. Якщо контролер або оператор, що не мають осідку в Союзі, опрацьовує персональні дані суб'єктів даних, які перебувають у Союзі, а опрацювання даних стосується надання товарів чи постачання послуг, незалежно від необхідності здійснення оплати суб'єктом даних таким суб'єктам даних у Союзі або моніторингу їхньої поведінки мірою вираження їхньої поведінки в Союзі, повинні призначити представника, за винятком ситуацій, коли опрацювання призначене для окремого випадку і передбачає опрацювання великих за обсягами масивів персональних даних спеціальних категорій або опрацювання персональних даних щодо судимостей і кримінальних злочинів, що, ймовірно, створить ризик для прав і свобод фізичних осіб, враховуючи специфіку, масштаб і цілі опрацювання, або якщо контролер є органом публічної влади. Представник повинен діяти від імені контролера або оператора, і до нього може звертатися будь-який наглядовий орган. Підставою для призначення представника слугує письмове доручення контролера або оператора. Призначення такого представника не впливає на обов'язки або відповідальність контролера або оператора, передбачені цим Регламентом. Представник повинен виконувати свої обов'язки згідно з повноваженнями, отриманими від контролера або оператора, в тому числі, співпрацюючи з компетентними наглядовими органами щодо будь-якої дії, вчиненої для забезпечення відповідності цьому Регламенту. На призначеного представника поширюється застосування виконавчого провадження у випадку порушень з боку контролера або оператора.

81. Для забезпечення дотримання вимог цього Регламенту щодо опрацювання, яке здійснюватиме оператор від імені контролера і за його дорученням, контролер повинен використовувати послуги лише таких операторів, які надають достатньо гарантій, зокрема, щодо експертних знань, надійності та ресурсів, для реалізації технічних і організаційних інструментів, які відповідатимуть вимогам цього Регламенту, в тому числі щодо безпеки опрацювання. Дотримання оператором затвердженого кодексу поведінки чи затвердженого механізму сертифікації можна вважати еле-

ментом підтвердження відповідності зобов'язанням контролера. Виконання операцій опрацювання оператором необхідно регулювати договором або іншим нормативно-правовим актом, згідно з законодавством Союзу або держави-члена, який окреслює зобов'язання оператора перед контролером, визначає предмет і тривалість опрацювання, специфіку і цілі опрацювання, тип персональних даних і категорії суб'єктів даних, з урахуванням спеціальних завдань і обов'язків оператора в контексті опрацювання, яке необхідно здійснити, та ризику для прав і свобод суб'єкта даних. Контролер і оператор можуть обрати індивідуальний договір або використовувати положення стандартного договору, ухваленого безпосередньо Комісією або спочатку наглядовим органом, а потім – Комісією. Завершивши опрацювання від імені контролера, оператор повинен, на розсуд контролера, повернути або вилучити персональні дані, за винятком випадку, коли відсутні вимоги щодо збереження персональних даних згідно з законодавством Союзу або держави-члена, яке поширюється на оператора.

82. Щоб довести відповідність цьому Регламенту, контролер і оператор повинні зберігати записи щодо опрацювання даних, здійсненого в межах їхніх обов'язків. Усі контролери й оператори зобов'язані співпрацювати з наглядовим органом і надавати йому ці записи на запит для сприяння моніторингу операцій опрацювання.

83. Для гарантування безпеки та запобігання опрацюванню, що порушує цей Регламент, контролер або оператор повинні оцінювати ризики, що супроводжують опрацювання, та вживати заходів для зниження таких ризиків, наприклад, вдаватися до шифрування. Такі заходи покликані гарантувати належний рівень безпеки, в тому числі конфіденційність, сучасний рівень розвитку та обґрунтованість витрат на їх реалізацію з урахуванням ризиків і специфіки персональних даних, що підлягають захисту. Оцінювати насамперед треба такі ризики, спричинені опрацюванням персональних даних, як випадкове чи незаконне знищення, втрата, зміна, несанкціоновані розкриття або доступ до персональних даних, які передають, зберігають або іншим чином опрацьовують, що, зокрема, можуть мати наслідком фізичну, матеріальну та нематеріальну шкоду.

84. Для підвищення ступеня відповідності цьому Регламенту в ситуаціях, коли операції опрацювання можуть спричинити високий ризик для прав і свобод фізичних осіб, контролер повинен нести відповідальність за проведення оцінювання впливу на захист даних з метою визначення, зокрема, походження, специфіки, особливості та ступеня тяжкості такого ризику. Результати оцінювання необхідно враховувати при визначенні заходів, яких необхідно вжити для підтвердження того, що опрацювання персональних даних відповідає цьому Регламенту. Якщо оцінка впливу на захист даних свідчить про те, що операції опрацювання містять високий ризик, який контролер не може знизити, через обмежені можливості технології та брак коштів, перед початком опрацювання необхідно проконсультуватися з наглядовим органом.

85. Порушення захисту персональних даних, якщо його не розглянути своєчасно і належним чином, може призвести до заподіяння фізичним особам фізичної, матеріальної та нематеріальної шкоди, зокрема до втрати контролю над їхніми персональними даними або обмеження їхніх прав, дискримінації, крадіжки персональних даних або шахрайства, фінансових втрат, несанкціонованого скасування використання псевдонімів, шкоди репутації, втрати конфіденційності персональних даних, захищених як особиста таємниця, або будь-якої іншої істотної економічної або соціальної шкоди фізичній особі. Отже, щойно контролеру стає відомо про порушення захисту персональних даних, він повинен повідомити про це наглядовий орган та, за можливості, не пізніше ніж за 72 години після того, як йому стало про це відомо, за винятком випадків, коли контролер може довести, згідно з принципом підзвітності, що ризик від порушення захисту персональних даних для прав і свобод фізичних осіб малоймовірний. Якщо здійснити таке повідомлення протягом 72 годин неможливо, то разом із повідомленням необхідно надати відомості про причини затримки; інформацію можна надати поетапно без подальших затримок.

86. Контролер повинен повідомити суб'єкту даних про порушення захисту його персональних даних без неналежної затримки, якщо таке порушення, ймовірно, загрожує високим ризиком для прав і свобод фізичної особи, щоб дозволити їй вжити необхідних запобіжних заходів. У повідомленні необхідно описати специфіку порушення захисту персональних даних, а також надати рекомендації щодо зменшення потенційних негативних наслідків. Такі повідомлення суб'єктам треба надіслати якомога швидше та в тісній співпраці з наглядовим органом, дотримуючись настанов, наданих ним або іншими відповідними органами, зокрема правоохоронними. Наприклад, потреба знизити безпосередній ризик заподіяння шкоди вимагає належної комунікації з суб'єктами даних, оскільки потреба в реалізації відповідних заходів проти тривалих або подібних порушень захисту персональних даних може бути підставою для необхідності додаткового часу для надання повідомлення.

87. Необхідно переконатися, чи були належно реалізовані всі заходи технологічного захисту та організаційні заходи для того, щоб з'ясувати, чи порушено захист персональних даних, а також чи повідомлено наглядовий орган і суб'єкта даних належним чином, без затримок. Необхідно також встановити, чи враховано в повідомленні специфіку і тяжкість порушення захисту персональних даних, його наслідки та негативний вплив на суб'єкта даних. Порушення вимог до повідомлення може спричинити втручання наглядового органу в межах його повноважень, передбачених цим Регламентом.

88. Вимоги до формату і процедур надання повідомлення про порушення захисту персональних даних передбачають аналіз наслідків такого порушення, в тому числі з'ясування того, чи перебували персональні дані під захистом відповідних заходів технічного захисту, що у дієвий спосіб

обмежують ймовірність крадіжки персональних даних або інші форми неправомірного використання. Крім того, у таких правилах і процедурах необхідно враховувати законні інтереси правоохоронних органів, якщо дострокове розкриття може невиправдано ускладнити розслідування обставин порушення захисту персональних даних.

89. Директивою 95/46/ЄС передбачено загальний обов'язок повідомляти наглядові органи про опрацювання персональних даних. Окрім того, що цей обов'язок спричиняє додаткове адміністративне і фінансове навантаження, він не обов'язково сприяє поліпшенню захисту персональних даних. Недискримінаційні загальні обов'язки щодо надання повідомлення необхідно скасувати та замінити дієвими процедурами і механізмами, що, натомість, зосереджуються на тих типах операцій опрацювання, які ймовірно створюють високий ризик для прав і свобод фізичних осіб через свої специфіку, масштаби, контекст і цілі. Такими типами операцій опрацювання можуть бути операції, які, зокрема, передбачають використання нових технологій або є новими і такими, щодо яких контролер раніше не провадив жодного оцінювання впливу на захист даних, або такими, що стають необхідними з урахуванням часу, що минув з моменту первинного опрацювання.

90. У таких випадках контролер повинен провести оцінювання впливу на захист даних до моменту опрацювання для того, щоб визначити ймовірність і ступінь тяжкості ризику, враховуючи специфіку, обсяг, контекст і цілі опрацювання та джерела ризику. У такій оцінці необхідно вказати, зокрема, заходи, гарантії та механізми, які спроможні знизити ризик, забезпечити захист персональних даних і не суперечать цьому Регламенту.

91. Це, зокрема, стосується масштабних операцій з опрацювання, значних обсягів персональних даних на регіональному, національному чи наднаціональному рівнях, які можуть одночасно вплинути на велику кількість суб'єктів даних і ймовірно створити високий ризик, наприклад, враховуючи їхню чутливість, а також інших операцій опрацювання, що створюють високий ризик для прав і свобод суб'єктів даних, зокрема, якщо такі операції ускладнюють реалізацію суб'єктами даних їхніх прав. Оцінювати вплив на захист даних також необхідно, якщо персональні дані опрацьовують з метою ухвалення рішень щодо певних фізичних осіб після будь-якого систематичного та всебічного оцінювання персональних аспектів, що стосуються фізичних осіб, на підставі профайлінгу таких даних чи після опрацювання спеціальних категорій персональних даних, біометричних даних або даних про судимості і кримінальні злочини чи пов'язані заходи безпеки. Оцінювання впливу на захист даних є однаково необхідним для всебічного моніторингу загальнодоступних територій, особливо при застосуванні оптико-електронних приладів або для будь-яких інших операцій, у ході виконання яких компетентний наглядовий орган вважає, що опрацювання ймовірно створить високий ризик для прав і свобод суб'єктів даних, зокрема, тому, що вони заважають суб'єктам даних реалізувати право або користуватися послугою чи договором, або тому, що

їх здійснюють систематично та масштабно. Опрацювання персональних даних не можна вважати масштабним, якщо воно стосується персональних даних пацієнтів або клієнтів, які надає персональний лікар, інший медичний працівник чи юрист. У таких випадках оцінювання впливу на захист даних не є обов'язковим.

92. За деяких обставин доцільним і раціональним для предмета оцінювання впливу на захист даних постає більш широке охоплення, аніж окремий проект, наприклад, коли органи публічної влади чи організації мають намір запровадити платформу єдиного застосування чи опрацювання або коли декілька контролерів планують створити єдине середовище застосування чи опрацювання в межах сектора чи сегмента промисловості або для горизонтальної діяльності широкої сфери застосування.

93. У контексті ухвалення нормативно-правового акта, що слугує основою для виконання завдань органом публічної влади і регулює конкретну операцію опрацювання чи низку відповідних операцій, держава-член може вважати за необхідне провести таке оцінювання перед початком опрацювання даних.

94. Якщо у ході оцінювання впливу на захист даних з'ясується, що опрацювання, за відсутності гарантій, заходів безпеки і механізмів зниження ризику, створює високий ризик для прав і свобод фізичних осіб, і контролер вважає, що ризик не можна знизити за допомогою наявних технологічних засобів і коштів, перед початком опрацювання даних необхідно проконсультуватися з наглядовим органом. Такий високий ризик, імовірно, характерний для окремих типів опрацювання даних, масштабів і періодичності опрацювання і може спричинити шкоду чи втручання в права і свободи фізичної особи. Наглядовий орган повинен відповісти на запит про надання консультації протягом визначеного строку. Проте відсутність реакції наглядового органу протягом такого строку не повинна обмежувати втручання наглядового органу, згідно з його завданнями та повноваженнями, передбаченими цим Регламентом, в тому числі повноваженням забороняти операції опрацювання. У ході консультаційного процесу стосовно оцінювання впливу на захист даних до наглядового органу можна подати інформацію про передбачені заходи зі зниження ризику для прав і свобод фізичних осіб.

95. Оператор повинен надавати допомогу контролеру, в разі необхідності та на запит, у виконанні обов'язків з оцінювання впливу на захист даних та в організації попередньої консультації з наглядовим органом.

96. Консультуватися з наглядовим органом необхідно також під час підготування законодавчого чи регуляторного інструментів, що передбачають опрацювання персональних даних, щоб забезпечити відповідність призначеного опрацювання цьому Регламенту та, зокрема, знизити ризики для суб'єкта даних.

97. Якщо опрацювання здійснює орган публічної влади, окрім судів або незалежних судових органів, що діють як судові органи, або якщо

в приватному секторі опрацювання здійснює контролер, до основних видів діяльності якого належать операції опрацювання, що вимагають регулярного, систематичного і широкомасштабного моніторингу суб'єктів даних, або якщо основні види діяльності контролера або оператора становлять широкомасштабне опрацювання спеціальних категорій персональних даних і даних про судимості і кримінальні злочини, у проведенні моніторингу внутрішньої відповідності цьому Регламенту контролеру або оператору повинна надавати допомогу особа, яка володіє експертними знаннями законодавства і процесуальних норм щодо захисту даних. У приватному секторі основні види діяльності контролера пов'язані з його первинними видами діяльності та не пов'язані з опрацюванням персональних даних як допоміжним видом діяльності. Необхідно визначити рівень експертних знань, зокрема, у сфері здійснюваних операцій опрацювання та захисту персональних даних. Фахівці з питань захисту даних, незалежно від того, чи є вони працівниками контролера, повинні мати можливість виконувати свої обов'язки та завдання у незалежний спосіб.

98. Необхідно заохочувати асоціації чи інші органи, що представляють категорії контролерів або операторів, розробляти кодекси поведінки, в межах цього Регламенту, для сприяння дієвому застосуванню цього Регламенту, враховуючи особливості опрацювання в окремих секторах, а також особливі потреби мікропідприємств, малих і середніх підприємств. Зокрема, такі кодекси поведінки покликані врегулювати обов'язки контролерів і операторів із урахуванням ризику, що ймовірно виникає внаслідок опрацювання, для прав і свобод фізичних осіб.

99. Укладаючи кодекс поведінки або вносячи зміни чи доповнення до такого кодексу, асоціації та інші органи, що представляють категорії контролерів або операторів, повинні консультуватися з відповідними стейкхолдерами, в тому числі суб'єктами даних, за можливості, та враховувати їхню думку.

100. Для посилення прозорості та узгодження з цим Регламентом необхідно заохочувати запровадження механізмів сертифікації та штампів і знаків захисту даних, що допомагатимуть суб'єктам даних швидко оцінювати ступінь захисту даних відповідних продуктів і сервісів.

101. Потоки персональних даних до країн і з країн поза межами Союзу та міжнародних організацій сприяють пожвавленню міжнародної торгівлі та міжнародної співпраці. Зростання таких потоків зумовило нові проблеми у сфері захисту персональних даних. Проте, якщо персональні дані передаються з Союзу до контролерів, операторів чи інших одержувачів у третіх країнах або до міжнародних організацій, рівень захисту фізичних осіб, який забезпечує в Союзі цей Регламент, не повинен бути ослабленим, у тому числі у випадках передавання персональних даних із третьої країни чи міжнародної організації до контролерів, операторів у тій самій чи іншій третій країні чи міжнародній організації. За будь-яких умов акти

передавання до третіх країн і міжнародних організацій повинні здійснюватися з дотриманням цього Регламенту.

102. Цей Регламент не порушує міжнародні угоди, укладені між Союзом і третіми країнами щодо передавання персональних даних, у тому числі щодо гарантій для суб'єктів даних. Держави-члени можуть укладати міжнародні угоди, що передбачають передавання персональних даних до третіх країн або міжнародних організацій, за умови, що такі угоди не суперечать цьому Регламенту або будь-яким іншим положенням законодавства Союзу та передбачають належний рівень захисту фундаментальних прав суб'єктів даних.

103. Комісія може ухвалити рішення, чинність якого поширюється на весь Союз, про те, що третя країна, територія, визначений сектор у межах третьої країни або міжнародна організація забезпечує належний рівень захисту даних, таким чином гарантуючи правову визначеність й однорідність у межах Союзу в тому, що стосується третьої країни чи міжнародної організації, що, як вважається, забезпечує такий рівень захисту. У таких випадках акти передавання персональних даних до третьої країни чи міжнародної організації можуть відбуватися без спеціального дозволу. Комісія може також ухвалити рішення про скасування, повідомивши та надавши третій країні чи міжнародній організації повний звіт із обґрунтуванням причин.

104. У світлі фундаментальних цінностей, на яких засновано Союз, зокрема, захисту прав людини, Комісія повинна у своїй оцінці третьої країни чи території або визначеного сектора в межах третьої країни враховувати те, як третя країна дотримується вимог верховенства права, доступу до правосуддя, а також міжнародних норм і стандартів прав людини, свого загального та секторального права, в тому числі законодавства щодо громадської безпеки, оборони та національної безпеки, а також публічного порядку і кримінального права. Під час ухвалення рішення про відповідність щодо території чи визначеного сектора в третій країні необхідно враховувати чіткі та об'єктивні критерії, такі як спеціальні види опрацювання даних і масштаб застосовуваних правових стандартів, а також чинне в третій країні законодавство. Третя країна повинна надати гарантії забезпечення належного рівня захисту, який суттєво відповідає забезпечуваному в межах Союзу, зокрема в разі опрацювання персональних даних в одному або декількох визначених секторах. Зокрема, третя країна повинна забезпечити дієвий незалежний нагляд за захистом даних і передбачити механізми співпраці з органами захисту даних держав-членів, а суб'єктам даних надати дієві права та дієві адміністративні і судові засоби правового захисту.

105. Крім міжнародних зобов'язань, які взяли на себе третя країна чи міжнародна організація, Комісія повинна враховувати зобов'язання, що виникають у ході участі третьої країни чи міжнародної організації в багатосторонній або регіональній системах, зокрема, в зв'язку з захистом персональних даних, а також виконання таких зобов'язань. Наприклад,

необхідно враховувати, чи приєдналася третя країна до Конвенції Ради Європи про захист фізичних осіб у зв'язку з автоматизованим опрацюванням персональних даних від 28 січня 1981 р. та її додаткових протоколів. Оцінюючи рівень захисту в третіх країнах або міжнародних організаціях, Комісія повинна консультуватися з Радою.

106. Комісія повинна відстежувати дієвість рішень щодо рівня захисту в третій країні, на території, у визначеному секторі в межах третьої країни або міжнародній організації та відстежувати дієвість рішень, ухвалених на підставі ст. 25 (6) або ст. 26 (4) Директиви 95/46/ЄС. У своїх рішеннях про відповідність Комісія повинна передбачити механізм періодичної перевірки їх дієвості. Таку періодичну перевірку необхідно провадити під час консультацій з відповідною третьою країною чи міжнародною організацією, враховуючи при цьому всі відповідні розробки в третій країні чи міжнародній організації. Провадячи моніторинг і періодичні перевірки, Комісія повинна враховувати думки та висновки Європейського Парламенту і Ради, а також інших відповідних органів і джерел, оцінювати, протягом розумного строку, дієвість останніх рішень і звітувати, згідно з Регламентом Європейського Парламенту і Ради (ЄС) № 182/2011*.

107. Комісія може визнати, що третя країна, територія, визначений сектор у межах третьої країни чи міжнародна організація більше не забезпечує належний рівень захисту даних. Відповідно, передавання персональних даних до такої третьої країни чи міжнародної організації необхідно заборонити, за винятком випадку, коли виконано вимоги цього Регламенту щодо актів передавання, що передбачають застосування відповідних гарантій, у тому числі зобов'язальних корпоративних правил, з дотриманням винятків щодо спеціальних ситуацій. У такому разі необхідно організувати консультації між Комісією та такими третіми країнами чи міжнародними організаціями. Комісія повинна своєчасно повідомити третю країну чи міжнародну організацію про причини та розпочати консультації з ними для того, щоб виправити ситуацію.

108. За відсутності рішення про відповідність контролер або оператор повинні вживати заходів для компенсації недостатнього захисту даних у третій країні шляхом застосування відповідних гарантій до суб'єкта даних. Такі відповідні гарантії можуть становити застосування зобов'язальних корпоративних правил, стандартних положень про захист даних, ухвалених Комісією, стандартних положень про захист даних, ухвалених наглядовим органом, або договірних положень, дозвіл на які надано наглядовим органом. Ці гарантії покликані забезпечувати відповідність вимогам до захисту даних і правам суб'єктів даних, що відповідають опрацюванню в межах Союзу, в тому числі наявність прав суб'єкта даних, які можна реалізувати, та дієвих засобів правового захисту, в тому числі на

* Регламент Європейського Парламенту і Ради (ЄС) № 182/2011 від 16 лютого 2011 р. про норми та загальні принципи механізмів контролю з боку держав-членів щодо реалізації Комісією виконавчих повноважень (ОВ L 55, 28.02.2011, с. 13).

отримання дієвих адміністративних чи судових засобів правового захисту та права вимоги відшкодування, в Союзі чи в третій країні. Вони повинні стосуватися, зокрема, відповідності загальним принципам щодо опрацювання персональних даних, принципам захисту даних за призначенням і за замовчуванням. Передавання також можуть здійснювати публічні органи до публічних органів у третіх країнах або міжнародних організацій з відповідними обов'язками чи функціями, в тому числі на підставі положень, що підлягають внесенню до таких адміністративних домовленостей, як меморандум про взаєморозуміння, що передбачають права, які можна реалізувати, та дієві права для суб'єктів даних. Якщо гарантії передбачені адміністративними домовленостями, що не мають зобов'язальної сили, необхідно отримати дозвіл компетентного наглядового органу.

109. Можливість контролера або оператора застосовувати стандартні положення про захист даних, ухвалені Комісією чи наглядовим органом, не повинні утримувати контролерів або операторів ані від внесення стандартних положень про захист даних у договір між оператором та іншим оператором, ані від їх доповнення положеннями або гарантіями за умови, що вони не суперечать, прямо чи опосередковано, договірним положенням, ухваленим Комісією чи наглядовим органом, або не обмежують фундаментальні права чи свободи суб'єктів даних. Необхідно заохочувати контролерів і операторів надавати додаткові гарантії у формі договірних зобов'язань, що доповнюють стандартні положення про захист.

110. Підприємства, які провадять спільну господарську діяльність, повинні мати можливість застосовувати зобов'язальні корпоративні правила для здійснення міжнародного передавання з Союзу до організацій у межах тієї самої групи підприємств або групи підприємств, що провадять спільну господарську діяльність, за умови, що такі корпоративні правила охоплюють усі суттєві принципи та права, які можна реалізувати, з метою надання відповідних гарантій для передавання або категорій передавання персональних даних.

111. Необхідно передбачити можливість передавання за певних обставин, коли суб'єкт даних надав свою чітку згоду, а передавання призначене для окремого випадку і є необхідним у зв'язку з договором або судовим позовом, незалежно від того, чи здійснюють його у порядку судової процедури, в адміністративному чи будь-якому позасудовому порядку, в тому числі в межах процедур регуляторних органів. Необхідно також передбачити можливість передавання у випадку, коли цього вимагають суспільні інтереси, встановлені законодавством Союзу чи держави-члена, чи коли передавання здійснюють з реєстру, запровадженого законом та призначеного для доступу громадськості чи осіб, що мають законний інтерес. В останньому випадку таке передавання не повинно поширюватися на всі персональні дані чи всі категорії даних реєстру, та, якщо реєстр призначений для доступу осіб, які мають законний інтерес, передавання необхідно здійснювати лише на запит таких осіб або, якщо вони повинні

бути одержувачами, повністю враховуючи інтереси та фундаментальні права суб'єкта даних.

112. Такі винятки необхідно, зокрема, застосовувати до передавання даних, що є необхідним для важливих цілей суспільного інтересу, наприклад у випадках міжнародного обміну даними між компетентними органами, податковими чи митними відомствами, між органами фінансового нагляду, між службами соціального забезпечення чи охорони суспільного здоров'я, наприклад, у випадку відстеження контактів осіб з інфекційними захворюваннями чи для того, щоб зменшити та/або викорінити допінг у спорті. Опрацювання персональних даних необхідно також розглядати як законне у випадку, коли необхідно захистити життєво важливі інтереси суб'єкта даних або іншої особи, в тому числі фізичну недоторканність або життя, якщо суб'єкт даних не спроможний надати згоду. За відсутності рішення про відповідність нормативно-правовий акт Союзу чи держави-члена може, з урахуванням суспільного інтересу, чітко встановлювати обмеження на передавання спеціальних категорій даних до третьої країни чи міжнародної організації. Держави-члени повинні повідомляти Комісію про такі положення. Будь-яке передавання персональних даних суб'єкта даних, який фізично чи юридично неспроможний надати згоду, до міжнародної гуманітарної організації з метою виконання завдання, покладеного Женевськими конвенціями, чи забезпечення відповідності нормам міжнародного гуманітарного права, застосовного в збройних конфліктах, можна вважати суспільно необхідним або таким, що відповідає життєво важливим інтересам суб'єкта даних.

113. Передавання, яке можна кваліфікувати як таке, що не повторюється і стосується лише обмеженої кількості суб'єктів даних, також відповідає законним інтересам контролера, якщо інтереси чи права та свободи суб'єкта даних не переважають над такими інтересами та якщо контролер оцінив усі обставини, пов'язані з передаванням даних. Контролер повинен приділити особливу увагу специфіці персональних даних, цілі та тривалості запропонованої операції чи операцій опрацювання, а також ситуації в країні походження, третій країні та країні кінцевого призначення та надати відповідні гарантії для захисту фундаментальних прав і свобод фізичних осіб у зв'язку з опрацюванням їхніх персональних даних. Таке передавання повинно бути можливим лише у виняткових випадках, коли жодна з інших підстав для передавання не є застосовною. Для цілей наукового, історичного дослідження або статистичних цілей необхідно враховувати правомірні очікування суспільства щодо підвищення рівня знань. Контролер повинен повідомити наглядовий орган і суб'єкта даних про факт передавання.

114. У будь-якому разі, якщо Комісія не ухвалює рішення щодо належного рівня захисту даних у третій країні, контролер або оператор повинні застосувати рішення, що забезпечують суб'єктів даних правами, які можна реалізувати, та дієвими правами щодо опрацювання їхніх даних у Союзі,

одразу після передавання таких даних для надання можливості подальшого отримання переваг від їхніх фундаментальних прав і гарантій.

115. Деякі треті країни ухвалюють закони, регламенти та інші нормативно-правові акти, призначені безпосередньо для врегулювання питання щодо опрацювання персональних даних фізичних і юридичних осіб, які перебувають під юрисдикцією держав-членів. Вони можуть включати рішення судів або трибуналів, рішення адміністративних органів у третіх країнах, що вимагають від контролера або оператора передати чи розкрити персональні дані, які ґрунтуються на міжнародній угоді, такій як договір про взаємну правову допомогу між третьою країною, яка подає запит, і Союзом або державою-членом. Екстериторіальна сфера застосування таких законів, регламентів та інших нормативно-правових актів може порушувати міжнародне право та ускладнювати досягнення цілей захисту фізичних осіб, гарантованих у Союзі цим Регламентом. Дозволено здійснювати лише ті передавання, під час яких дотримуються умови цього Регламенту щодо передавання до третіх країн. Це може мати місце тоді, коли розкриття є необхідним для задоволення суспільних інтересів, визнаних законодавством Союзу чи держави-члена, сфера застосування якого поширюється на контролера.

116. Якщо персональні дані перетинають кордони за межами Союзу, це може створювати для фізичних осіб ризики в реалізації права захисту даних, зокрема, захисту від незаконного використання чи розкриття такої інформації. Водночас наглядові органи можуть визнати свою неспроможність розглядати скарги чи розслідувати види діяльності, які провадяться поза їхніми кордонами. Їхню співпрацю в транскордонному контексті можуть також ускладнювати обмежені повноваження, недосконалі нормативно-правові режими, брак ресурсів. Щоб співпраця в обміні інформацією та проведенні розслідувань між органами, які здійснюють нагляд за захистом даних, з їхніми міжнародними партнерами була ефективною, необхідно розробити механізм надання міжнародної допомоги в забезпеченні виконання положень законодавства щодо захисту персональних даних. Комісія та наглядові органи повинні обмінюватися інформацією та співпрацювати з компетентними органами третіх країн за принципом взаємності та згідно з цим Регламентом.

117. Створення у державах-членах наглядових органів з правом незалежного виконання своїх завдань і повноважень є істотним компонентом захисту прав фізичних осіб, пов'язаних з опрацюванням їхніх персональних даних. Держави-члени повинні мати можливість створювати декілька наглядових органів відповідно до їх конституційної, організаційної та адміністративної структури.

118. Незалежність наглядових органів не означає, що їх фінансові витрати не підлягають контролю чи моніторингу або судовій перевірці.

119. Якщо держава-член засновує декілька наглядових органів, вона повинна в законодавчому порядку запровадити механізми забезпечення

результативної участі таких наглядових органів у механізмі послідовності. Держава-член повинна, зокрема, призначити наглядовий орган, що діятиме як центр координації діяльності таких органів, їх співпраці з іншими наглядовими органами, Радою і Комісією.

120. Кожному наглядовому органу необхідно надати фінансові та людські ресурси, приміщення та інфраструктуру, необхідні для результативного виконання ними своїх завдань, у тому числі тих, що пов'язані зі взаємною допомогою та співпрацею з іншими наглядовими органами в межах Союзу. Кожний наглядовий орган повинен мати окремий публічний річний бюджет, що може бути складовою загальнодержавного або національного бюджету.

121. Принципи і правила діяльності члена чи членів наглядового органу повинні бути запроваджені в кожній державі-члені у законодавчому порядку; зокрема, вони повинні гарантувати призначення таких членів на основі прозорої процедури парламентом, урядом або очільником держави в державі-члені на підставі пропозиції, внесеної урядом, членом уряду, парламентом чи палатою парламенту, або незалежним органом, з відповідними повноваженнями, передбаченими законодавством держави-члена. Щоб забезпечити незалежність наглядового органу, його член або члени повинні діяти добросовісно, утримуватися від будь-яких дій, не сумісних з іншими їхніми обов'язками, протягом строку своїх повноважень, не провадити жодну іншу несумісну діяльність, прибуткову чи ні. Наглядовий орган повинен мати власний персонал, відібраний наглядовим органом або незалежним органом на підставі законодавства держави-члена, який повинен підпорядковуватися безпосередньому керівництву наглядового органу.

122. Кожний наглядовий орган повинен володіти компетенцією на території своєї держави-члена, достатньою для реалізації повноважень і виконання завдань, покладених на нього, згідно з цим Регламентом. Вона повинна охоплювати, зокрема, опрацювання в контексті діяльності осідку контролера або оператора на території своєї держави-члена, опрацювання персональних даних, яке здійснюють публічні органи чи публічні органи, що діють у межах суспільного інтересу, опрацювання, яке впливає на суб'єктів даних на його території, чи опрацювання, яке провадять контролер або оператор, які не мають осідку в Союзі, але воно спрямоване на суб'єктів даних, які проживають на його території. Це повинно включати розгляд скарг, поданих суб'єктом даних, провадження розслідувань щодо застосування цього Регламенту та сприяння громадській обізнаності про ризики, правила, гарантії та права, пов'язані з опрацюванням персональних даних.

123. Наглядові органи повинні здійснювати моніторинг застосування положень відповідно до цього Регламенту та сприяти його послідовному застосуванню в межах Союзу для того, щоб захистити права фізичних осіб, пов'язані з опрацюванням їхніх персональних даних, і сприяти вільному переміщенню персональних даних у межах внутрішнього ринку. З цією

метою наглядові органи повинні співпрацювати один з одним і з Комісією, за потреби, в будь-якій угоді між державами-членами щодо надання взаємної допомоги чи щодо такої співпраці.

124. Якщо опрацювання персональних даних відбувається в контексті діяльності осідку контролера або оператора в Союзі, а контролер або оператор мають осідки більше ніж в одній державі-члені, або якщо опрацювання, що відбувається в контексті діяльності єдиного осідку контролера чи оператора в Союзі, істотно впливає чи ймовірно істотно вплине на суб'єктів даних у більш ніж одній державі-члені, наглядовий орган за головним осідком контролера або оператора чи за єдиним осідком контролера або оператора повинен діяти як керівний орган. Він повинен співпрацювати з іншими відповідними органами, оскільки контролер або оператор має осідок на території їхньої держави-члена, оскільки суб'єкти даних, що проживають на їхній території, зазнають істотного впливу або тому, що до них було подано скаргу. Також, якщо суб'єкт даних, який не проживає в цій державі-члені, подав скаргу, наглядовий орган, до якого було подано таку скаргу, повинен також діяти як відповідний наглядовий орган. Рада повинна мати можливість видавати настанови, зокрема, щодо критеріїв, які необхідно враховувати для того, щоб переконатися, чи має відповідне опрацювання істотний вплив на суб'єктів даних у декількох державах-членах, а також щодо того, що становить відповідне та обґрунтоване заперечення.

125. Керівний орган повинен бути уповноваженим на ухвалення зобов'язальних рішень щодо завдань, покладених на нього цим Регламентом. Як керівний орган наглядовий орган повинен активно залучати інші наглядові органи до процесу вироблення й ухвалення рішень. Якщо рішення полягає у відхиленні скарги, поданої суб'єктом даних, ухвалити його повинен наглядовий орган, до якого подано скаргу.

126. Узгоджене з керівним наглядовим органом рішення відповідного наглядового органу надсилають до головного або єдиного осідку контролера чи оператора. Контролер або оператор повинні вживати усіх необхідних заходів для виконання рішення відповідно до цього Регламенту.

127. Кожний наглядовий орган, що не є керівним наглядовим органом, має право розглядати місцеві справи, якщо контролер або оператор мають осідки більше ніж в одній державі-члені, а предмет спеціального опрацювання стосується лише опрацювання, яке здійснюють в одній державі-члені із залученням лише суб'єктів даних цієї держави-члена, наприклад, якщо предмет стосується опрацювання персональних даних працівників у спеціальному контексті зайнятості в межах держави-члена. У таких випадках наглядовий орган повинен одразу інформувати керівний наглядовий орган про суть питання, а керівний наглядовий орган на підставі цієї інформації повинен вирішити, чи розглядатиме він справу відповідно до положення про співпрацю між керівним наглядовим органом та іншими відповідними наглядовими органами (механізм «єдиного вікна»), чи справу розглядатиме на місцевому рівні наглядовий орган,

який про неї повідомив. Ухвалюючи рішення про те, хто розглядатиме справу, керівний наглядовий орган повинен врахувати, чи має контролер або оператор осідок у державі-члені наглядового органу, який про це повідомив. Якщо керівний наглядовий орган вирішує розглядати справу самостійно, наглядовий орган, який повідомив про неї, повинен мати можливість подати проект рішення, на який керівний наглядовий орган повинен звернути максимальну увагу, готуючи свій проект рішення в межах зазначеного механізму єдиного вікна.

128. Правила щодо керівного наглядового органу та механізму єдиного вікна не можна застосовувати, якщо опрацювання здійснюють публічні органи чи приватні органи для задоволення суспільного інтересу. У таких випадках єдиним наглядовим органом, повноваження на якого покладені цим Регламентом, повинен бути наглядовий орган держави-члена, в якій засновано публічний орган або приватний орган.

129. Для забезпечення послідовного моніторингу і виконання цього Регламенту в межах Союзу наглядові органи в різних державах-членах повинні мати однакові завдання та дієві повноваження, в тому числі повноваження на розслідування, виправні повноваження та санкції, дозвільні та консультативні повноваження, зокрема, у випадках подання скарг фізичними особами, і без обмеження повноважень органів прокуратори, за законодавством держави-члена, доводити інформацію про порушення цього Регламенту до відома судових органів і брати участь у судовому процесі. Такі повноваження повинні також включати повноваження накладати тимчасові або остаточні обмеження, в тому числі заборону, на опрацювання. Держави-члени мають право визначати інші завдання, пов'язані з захистом персональних даних і передбачені цим Регламентом. Повноваження наглядових органів необхідно реалізувати відповідно до належних процедурних гарантій, встановлених законодавством Союзу та держави-члена, неупереджено, правомірно та в розумний строк. Зокрема, кожен захід має бути доцільним, необхідним і пропорційним в аспекті забезпечення відповідності цьому Регламенту, з огляду на обставини кожної індивідуальної справи, поважати право кожної особи бути вислуханою перед вжиттям будь-якого індивідуального заходу, що може негативно вплинути на неї, та уникати зайвих витрат і надмірних незручностей для відповідних осіб. Слідчі повноваження щодо доступу до приміщень необхідно реалізувати відповідно до спеціальних вимог процесуального права держави-члена, зокрема, вимоги отримання попереднього судового дозволу. Кожний юридично зобов'язальний інструмент наглядового органу має бути сформульований у письмовій формі, чітко й однозначно, із зазначенням наглядового органу, який його ухвалив, дати ухвалення інструменту, повинен містити підпис голови чи члена наглядового органу, уповноваженого ним, обґрунтування інструменту, а також вказувати на право щодо дієвого засобу правового захисту. Це не виключає можливих додаткових вимог, згідно з процесуальним правом держави-члена. Ухвалення юридично зобов'язаль-

ного рішення передбачає, що воно може призвести до судового перегляду в державі-члені наглядового органу, який ухвалив рішення.

130. Якщо наглядовий орган, до якого подано скаргу, не є керівним наглядовим органом, керівний наглядовий орган повинен тісно співпрацювати з наглядовим органом, до якого подано скаргу, згідно з положеннями щодо співпраці та послідовності, викладеними в цьому Регламенті. У таких випадках керівний наглядовий орган повинен, вживаючи заходів, які матимуть правові наслідки, у тому числі накладаючи адміністративні штрафи, максимально враховувати думку наглядового органу, до якого подано скаргу та який володітиме повноваженнями на проведення будь-якого розслідування на території своєї держави-члена у взаємодії з компетентним наглядовим органом.

131. Якщо наглядовий орган має статус керівного наглядового органу щодо оператора або процесора, але конкретний предмет скарги чи можливе порушення стосується лише опрацювання даних, яке здійснює оператор або процесор у державі-члені, де подано скаргу або виявлено можливе порушення, а справа не впливає істотно чи ймовірно істотно не впливатиме на суб'єктів даних в інших державах-членах, наглядовий орган, що отримує скаргу чи виявляє ситуацію або якого повідомлено іншим чином про ситуації, що тягнуть за собою можливі порушення цього Регламенту, повинен прагнути укладення мирової угоди з контролером і, якщо зробити це не вдасться, реалізувати повний спектр його повноважень, що охоплюють спеціальне опрацювання на території держави-члена наглядового органу чи щодо суб'єктів даних на території тієї держави-члена; опрацювання в контексті пропонування товарів або послуг, спеціально призначених для суб'єктів даних на території держави-члена наглядового органу; чи опрацювання, що має бути оцінене, виходячи з відповідних передбачених законодавством держави-члена зобов'язань.

132. Діяльність з підвищення рівня обізнаності громадськості, яку провадять наглядові органи, повинна передбачати спеціальні заходи, спрямовані на контролерів і операторів, у тому числі мікропідприємств, малих і середніх підприємств, а також фізичних осіб, зокрема, в освітньому контексті.

133. Наглядові органи повинні сприяти один одному у виконанні завдань і надавати допомогу для того, щоб забезпечити послідовне застосування та виконання цього Регламенту на внутрішньому ринку. Наглядовий орган, що надсилає запит про взаємну допомогу, не отримавши відповіді на запит про взаємну допомогу протягом одного місяця, може ухвалювати рішення про застосування тимчасового інструменту.

134. Кожний наглядовий орган повинен, за необхідності, брати участь у спільних операціях з іншими наглядовими органами. Наглядовий орган, який отримав запит, зобов'язаний відповісти на запит протягом визначеного періоду часу.

135. Для забезпечення послідовного застосування цього Регламенту в межах Союзу необхідно запровадити механізм послідовності співпраці

між наглядовими органами. Такий механізм, зокрема, застосовують, якщо наглядовий орган має намір ухвалити інструмент, спрямований на створення правових наслідків щодо операцій опрацювання, які істотно впливають на значну кількість суб'єктів даних у декількох державах-членах. Його необхідно також застосовувати, якщо будь-який відповідний наглядовий орган або Комісія надсилає запит про те, що справу необхідно розглядати згідно з механізмом послідовності. Такий механізм не повинен обмежувати будь-які заходи, які Комісія може вживати, реалізуючи свої повноваження за угодами.

136. Застосовуючи механізм послідовності, Рада повинна протягом визначеного періоду часу ухвалити висновок, якщо так вирішить більшість її членів або якщо існує запит відповідного наглядового органу чи Комісії. Рада повинна також мати повноваження на ухвалення юридично зобов'язальних рішень у разі виникнення суперечок між наглядовими органами. Такі юридично зобов'язальні рішення вона повинна ухвалювати, як правило, більшістю в дві третини голосів своїх членів, в чітко окреслених ситуаціях, якщо думки наглядових органів, зокрема, стосовно механізмів послідовності між керівним наглядовим органом і відповідними наглядовими органами не збігаються за суттю, зокрема щодо порушення цього Регламенту.

137. Може постати нагальна потреба діяти з метою захисту прав і свобод суб'єктів даних, зокрема якщо виникає загроза того, що реалізація права суб'єкта даних може бути істотно ускладнена. Наглядовий орган повинен, таким чином, бути спроможним ухвалювати рішення про застосування належним чином обґрунтованих тимчасових інструментів на своїй території з визначеним строком дії, що не перевищує трьох місяців.

138. Застосування такого механізму повинно бути умовою законності інструменту, спрямованого на породження наглядовим органом правових наслідків у тих випадках, коли його застосування є обов'язковим. В інших випадках транскордонного значення необхідно застосовувати механізм співпраці керівного наглядового органу і відповідних наглядових органів, а спільно надавати допомогу і здійснювати операції можуть відповідні наглядові органи на двосторонній чи багатосторонній основі без застосування механізму послідовності.

139. Щоб сприяти послідовному застосуванню цього Регламенту, Рада має бути незалежним органом Союзу і володіти правосуб'єктністю. Раду очолює Голова. Вона створена замість Робочої групи із захисту осіб у сфері опрацювання персональних даних, заснованої Директивою 95/46/ЄС. До її складу входять голова наглядового органу кожної держави-члена та Європейський інспектор із захисту даних або їхні відповідні представники. Комісія бере участь у діяльності Ради без права голосу, а Європейський інспектор із захисту даних має особливе право голосу. Рада покликана сприяти послідовному застосуванню цього Регламенту в межах Союзу, в тому числі надаючи консультації Комісії, зокрема, щодо рівня захисту в

третіх країнах або міжнародних організаціях, та сприяючи співпраці наглядових органів у межах Союзу. Під час виконання своїх завдань Рада діє незалежно.

140. Раді зобов'язаний допомагати секретаріат, який забезпечує Європейський інспектор із захисту даних. Персонал Європейського інспектора із захисту даних, залучений до виконання завдань, покладених на нього радою, згідно з цим Регламентом, повинен виконувати свої завдання виключно за дорученням Голови Ради та звітуючи їй.

141. Кожний суб'єкт даних повинен мати право подати скаргу до єдиного наглядового органу, зокрема, в державі-члені за місцем свого постійного проживання, та право на дієві засоби судового захисту, згідно зі ст. 47 Хартії, якщо суб'єкт даних вважає, що його або її права за цим Регламентом порушено, або якщо наглядовий орган не розглядає скаргу, частково чи повністю відхиляє її, відмовляє в розгляді скарги або демонструє бездіяльність у ситуації, яка вимагає вжиття заходів для захисту прав суб'єкта даних. Після отримання скарги повинно бути проведене розслідування, що підлягає судовому перегляду, тією мірою, що є необхідною для конкретної справи. Наглядовий орган повинен повідомити суб'єкта даних про стан і результати розгляду скарги протягом розумного строку. Якщо справа потребує подальшого розслідування чи координації з іншим наглядовим органом, суб'єкту даних необхідно надати попередню інформацію про це. Щоб спростити процес подання скарг, кожний наглядовий орган повинен вживати заходів, наприклад, розробити електронну форму скарги чи запропонувати застосування інших засобів зв'язку.

142. Якщо суб'єкт даних вважає, що його або її права за цим Регламентом порушено, він або вона повинні мати право уповноважити неприбутковий орган, організацію чи асоціацію, створені на підставі законодавства держави-члена, з метою виконання суспільно важливих завдань у сфері захисту персональних даних, подати до наглядового органу скаргу від його або її імені, реалізувати право на засоби судового захисту від імені суб'єктів даних або, якщо це передбачено законодавством держави-члена, реалізувати право на отримання відшкодування від імені суб'єктів даних. Держава-член може надати такому органу, організації чи асоціації право подати скаргу в такій державі-члені, незалежно від мандату суб'єкта даних, і право на дієві засоби судового захисту, якщо вона має підстави вважати, що права суб'єкта даних було порушено внаслідок опрацювання персональних даних з порушенням положень цього Регламенту. Такий орган, організація чи асоціація не можуть вимагати компенсації від імені суб'єкта даних незалежно від мандату суб'єкта даних.

143. Будь-яка фізична чи юридична особа має право подавати позов за анулювання рішень Ради до Суду на умовах, передбачених ст. 263 ДФЄС. Як адресати таких рішень зацікавлені наглядові органи, що бажають їх оскаржити, повинні подати позов протягом двох місяців після того, як їх повідомлено про них, згідно зі ст. 263 ДФЄС. У разі, якщо рішення ради

безпосередньо та в індивідуальному порядку стосуються контролера, оператора чи заявника, останній може подати позов на анулювання таких рішень протягом двох місяців з дати їх опублікування на офіційній сторінці Ради в мережі Інтернет, згідно зі ст. 263 ДФЄС. Без обмеження цього права, відповідно до ст. 263 ДФЄС, кожна фізична чи юридична особа повинна мати дієвий засіб судового захисту в компетентному національному суді щодо рішення наглядового органу, яке породжує правові наслідки щодо такої особи. Таке рішення стосується, зокрема, реалізації слідчих, виправних і дозвільних повноважень наглядовим органом або відхилення чи відмови у задоволенні скарг. Проте право на дієвий засіб судового захисту не передбачає заходів, яких вживають наглядові органи та які не є юридично зобов'язальними, наприклад, ухвалення висновків або надання наглядовим органом консультацій. Провадження щодо наглядового органу має відбуватися в судах держави-члена, де створено наглядовий орган, та відповідно до процесуального права тієї держави-члена. До юрисдикції таких судів належить розгляд усіх питань факту та права, які стосуються відповідного спору.

У разі відмови у задоволенні скарги чи її відхилення наглядовим органом заявник може звернутися до судів тієї самої держави-члена. У контексті засобів судового захисту, що стосуються застосування цього Регламенту, національні суди, які ухвалюють рішення з питання, необхідного для надання їм повноваження винести рішення, можуть, або у випадку, передбаченому ст. 267 ДФЄС, повинні, надіслати запит до Суду про винесення попередньої ухвали щодо тлумачення нормативно-правового акта Союзу, в тому числі цього Регламенту. Крім того, якщо рішення наглядового органу, на підставі якого виконується рішення ради, оскаржують у національному суді, а законність рішення ради спірна, національний суд не має повноваження оголошувати рішення ради незаконним, повинен передати питання щодо законності до Суду, згідно зі ст. 267 ДФЄС, відповідно до тлумачення Суду, якщо він вважає рішення незаконним. Проте національний суд може не передавати питання щодо законності рішення ради на запит фізичної чи юридичної особи, яка мала можливість подавати позов на анулювання такого рішення, особливо, якщо таке рішення безпосередньо стосувалося її особисто, але не зробила цього протягом строку, передбаченого ст. 263 ДФЄС.

144. Якщо суд, який розпочав провадження щодо рішення наглядового органу, має підстави вважати, що провадження щодо того самого опрацювання, зокрема, того самого предмета, що стосується опрацювання тим самим контролером або оператором, або тієї самої підстави для подання позову, передають до компетентного суду в іншій державі-члені, він повинен звернутися до такого суду для того, щоб підтвердити факт такого суміжного провадження. Якщо суміжне провадження перебуває на розгляді в суді в ще одній державі-члені, будь-який суд, що не є судом, який першим розпочав провадження, може продовжити провадження або, на запит однієї

зі сторін, відмовитися від юрисдикції на користь суду, який першим розпочав провадження, якщо такий суд має юрисдикцію щодо відповідного провадження і об'єднання таких суміжних проваджень дозволено його законодавством. Провадження вважаються суміжними, якщо вони пов'язані настільки тісно, що їх спільний розгляд і вирішення стають доцільними для уникнення ризику ухвалення суперечливих рішень, винесених у межах окремих проваджень.

145. У провадженні щодо контролера або оператора заявник повинен мати вибір щодо подання позову або до судів держав-членів, де має осідок контролер або оператор, або до судів держав-членів, в яких проживає суб'єкт даних, за винятком випадку, коли контролер є публічним органом держави-члена, що виконує свої публічні повноваження.

146. Контролер або оператор зобов'язаний відшкодувати будь-яку шкоду, заподіяну особі внаслідок опрацювання із порушенням цього Регламенту. Контролер або оператор мають бути звільнені від відповідальності, якщо буде доведено, що вони жодним чином не несуть відповідальності за заподіяну шкоду. Поняття шкоди необхідно тлумачити у широкому сенсі, в світлі прецедентного права Суду у спосіб, що повністю відображає цілі цього Регламенту. Воно не обмежує будь-які позови про відшкодування шкоди, що виникають внаслідок порушення інших норм нормативно-правового акта Союзу чи держави-члена. Опрацювання, що порушує цей Регламент, також означає опрацювання, що порушує делеговані акти та імплементаційні акти, ухвалені згідно з цим Регламентом і нормативно-правовим актом держави-члена, який уточнює норми цього Регламенту. Суб'єкти даних повинні отримати повне та результативне відшкодування за заподіяну їм шкоду. У разі залучення контролерів або операторів до того самого опрацювання, кожний контролер або оператор повинен нести відповідальність за заподіяння шкоди у повному обсязі, проте за їхньої спільної участі в одному провадженні, згідно із законодавством держави-члена, відшкодування може бути розподілено з урахуванням відповідальності кожного за шкоду, заподіяну внаслідок опрацювання, за умови забезпечення в повному обсязі результативного відшкодування суб'єкту даних, якому заподіяно шкоду. Будь-який контролер або оператор, що виплатив відшкодування у повному обсязі, може, відповідно, розпочати процедуру оскарження щодо інших контролерів або операторів, залучених до того самого опрацювання.

147. Якщо цей Регламент містить спеціальні норми щодо юрисдикції, зокрема, в частині провадження, у питанні судового засобу правового захисту, в тому числі відшкодування, щодо контролера або оператора, загальні норми щодо юрисдикції, наприклад, норми Регламенту Європейського Парламенту і Ради (ЄС) № 1215/2012*, не повинні обмежувати застосування таких спеціальних норм.

---

* Регламент Європейського Парламенту і Ради (ЄС) № 1215/2012 від 12 грудня 2012 р. про юрисдикцію, визнання і забезпечення виконання рішень у цивільних і комерційних справах (OB L 351, 20.12.2012, с. 1).

148. З метою розширення сфери застосування норм цього Регламенту, санкції, в тому числі адміністративні штрафи, необхідно накладати за будь-яке порушення цього Регламенту, окрім (або замість) заходів, застосованих наглядовим органом відповідно до цього Регламенту. У разі незначного порушення або якщо штраф, який ймовірно буде накладено, становитиме для фізичної особи надмірний тягар, замість штрафу можна винести догану. Необхідно належним чином враховувати специфіку, тяжкість і тривалість порушення, навмисний характер порушення, дії, яких було вжито для пом'якшення заподіяної шкоди, ступінь відповідальності чи будь-які відповідні попередні порушення, спосіб, у який наглядовий орган дізнався про порушення, відповідність інструментам, передбаченим щодо контролера або оператора, дотримання кодексу поведінки та будь-які інші обтяжувальні чи пом'якшувальні фактори. На накладення штрафів, у тому числі адміністративних, повинні поширюватися процесуальні гарантії, згідно із загальними принципами законодавства Союзу та Хартії, в тому числі дієвий судовий захист і належна правова процедура.

149. Держави-члени повинні мати можливість запроваджувати норми щодо кримінальних покарань за порушення цього Регламенту, в тому числі за порушення національних норм, ухвалених з урахуванням обмежень цього Регламенту. До таких кримінальних покарань може також бути віднесене позбавлення переваг, отриманих внаслідок порушення цього Регламенту. Проте призначення кримінальних покарань за порушення національних правил та адміністративних санкцій не повинно суперечити принципу *ne bis in idem* у тлумаченні Суду.

150. Щоб посилити та гармонізувати адміністративні санкції за порушення цього Регламенту, кожний наглядовий орган повинен мати повноваження накладати адміністративні штрафи. Цей Регламент визначає порушення і верхню межу та критерії накладання пов'язаних адміністративних штрафів, які має використовувати компетентний наглядовий орган у кожному окремому випадку, враховуючи всі обставини конкретної ситуації, зокрема, специфіку, тяжкість, тривалість порушення, його наслідки та інструменти, застосовані для забезпечення відповідності обов'язкам за цим Регламентом та запобігання чи пом'якшення наслідків порушення. Якщо адміністративні штрафи накладено на підприємство, його необхідно розуміти як підприємство, згідно зі ст. 101 і 102 ДФЄС для цих цілей. Якщо адміністративні штрафи накладено на осіб, що не є підприємством, наглядовий орган, визначаючи розмір штрафу, повинен враховувати загальний рівень доходу в державі-члені, а також матеріальне становище особи. Механізм послідовності також можна використовувати для сприяння послідовному застосуванню адміністративних штрафів. Саме держави-члени мають визначити, чи підлягають органи публічної влади накладенню адміністративних штрафів та якою мірою. Накладення адміністративного штрафу чи попередження про нього не впливають на застосування інших повноважень наглядових органів або інших санкцій за цим Регламентом.

151. Правові системи Данії та Естонії не передбачають накладення адміністративних штрафів, визначених у цьому Регламенті. Правила щодо адміністративних штрафів можна застосовувати у спосіб, аналогічний практиці Данії, де компетентні національні суди накладають штраф як кримінальне покарання, та – Естонії, де штраф накладає наглядовий орган у межах процедури покарання за незначні правопорушення, за умови, що таке застосування правил у державах-членах має наслідки, аналогічні накладенню адміністративних штрафів наглядовими органами. При цьому компетентні національні суди повинні враховувати рекомендацію наглядового органу, який порушує питання про стягнення штрафу. У будь-якому разі накладені штрафи повинні бути дієвими, пропорційними і стримувальними.

152. Якщо цей Регламент не гармонізує адміністративні санкції чи, за необхідності в інших випадках, наприклад, у разі серйозних порушень цього Регламенту, держави-члени повинні забезпечувати застосування системи, що передбачає дієві, пропорційні та стримувальні санкції. Сутність таких санкцій, кримінальних чи адміністративних, визначає законодавство держави-члени.

153. Держави-члени повинні узгоджувати норми, що регулюють свободу виявлення поглядів і свободу інформації, в тому числі журналістику, наукову, художню чи літературну діяльність, із правом на захист персональних даних відповідно до цього Регламенту. На опрацювання персональних даних винятково для цілей журналістики чи цілей наукової, художньої чи літературної діяльності повинна поширюватися чинність винятків з деяких положень цього Регламенту, якщо це необхідно для узгодження права на захист персональних даних із правом на свободу виявлення поглядів і свободу інформації, закріплених у ст. 11 Хартії. Це стосується, зокрема, опрацювання персональних даних у сфері аудіовізуальних послуг, архівах новин і бібліотеках. Тому держави-члени повинні ухвалити законодавчі інструменти, що встановлюють винятки, необхідні для узгодження фундаментальних прав. Держави-члени повинні ухвалити винятки із загальних принципів, прав суб'єкта даних, контролера і оператора, передавання персональних даних до третіх країн чи міжнародних організацій, незалежних наглядових органів, співпраці і послідовності, спеціальних ситуацій з опрацювання даних. Якщо такі винятки відрізняються в декількох державах-членах, необхідно застосовувати законодавство держави-члени, яке поширюється на контролера. Щоб врахувати важливість права на свободу виявлення поглядів у кожному демократичному суспільстві, поняття такої свободи, наприклад у журналістиці, необхідно тлумачити у широкому сенсі.

154. Цей Регламент передбачає врахування принципу публічного доступу до офіційних документів під час його застосування. Публічний доступ до офіційних документів можна вважати таким, що відповідає суспільним інтересам. Необхідно забезпечити можливість публічного розкриття персо-

нальних даних, що містяться в документах, які зберігає публічний орган або організація, таким органом або організацією, якщо таке розкриття передбачене законодавством Союзу чи держави-члена, що поширюється на публічний орган чи організацію. Таке законодавство повинно узгодити питання публічного доступу до офіційних документів і повторного використання інформації публічної сфери із правом на захист персональних даних, і, відтак, передбачивши узгодження з правом на захист персональних даних відповідно до цього Регламенту. Покликання на публічні органи та організації має в такому контексті включати усі органи чи інші організації, на які поширюється чинність законодавства держави-члена про публічний доступ до документів. Директива Європейського Парламенту і Ради 2003/98/ЄС* залишає без змін і жодним чином не впливає на рівень захисту фізичних осіб у зв'язку з опрацюванням персональних даних, окреслених положеннями законодавства Союзу чи держави-члена, та, зокрема, не змінює обов'язки та права, встановлені цим Регламентом. Зокрема, цю Директиву не застосовують до документів, доступ до яких виключено чи обмежено в силу режимів доступу на підставах захисту персональних даних, і частин документів, доступ до яких дозволено в силу таких режимів, що містять персональні дані, повторне використання яких передбачено на законодавчому рівні як таке, що несумісне із законодавством щодо захисту фізичних осіб у зв'язку з опрацюванням персональних даних.

155. У законодавстві держави-члена чи колективних угодах, в тому числі «трудових договорах», можуть бути передбачені спеціальні норми щодо опрацювання персональних даних працівників у контексті зайнятості, зокрема, умови, за яких персональні дані в контексті зайнятості можна опрацьовувати на підставі згоди працівника, цілі працевлаштування, виконання трудового договору, в тому числі виконання обов'язків, установлених законом або колективними угодами, управління, планування та організації праці, рівності та різноманітності на робочому місці, здоров'я та безпеки на робочому місці, для цілей реалізації та користування, індивідуально чи колективно, правами та перевагами, пов'язаними із зайнятістю, та для цілей припинення трудових відносин.

156. Опрацювання персональних даних для задоволення суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей повинно передбачати дотримання відповідних гарантій для прав і свобод суб'єкта даних, відповідно до цього Регламенту. Такі гарантії покликані забезпечувати наявність технічних і організаційних інструментів для гарантування, зокрема, принципу мінімізації даних. Подальше опрацювання персональних даних для цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей потрібно здійснювати, якщо контролер оцінив можливість реалізації таких цілей

* Директива Європейського Парламенту і Ради 2003/98/ЄС від 17 листопада 2003 р. про повторне використання інформації публічного сектора (OB L 345, 31.12.2003, с. 90).

за допомогою опрацювання даних, що не дозволяє чи більше не дозволяє ідентифікації суб'єктів даних, за умови, що існують відповідні гарантії (такі як використання псевдонімів). Держави-члени повинні передбачити відповідні гарантії для опрацювання персональних даних з метою задоволення суспільних інтересів, цілей наукового та історичного дослідження або статистичних цілей. Держав-членів необхідно уповноважити, за спеціальних умов і з урахуванням відповідних гарантій для суб'єктів даних, на уточнення виправлення, заповнення та скорочення вимог до інформації, обмеження опрацювання, мобільності даних і заперечення, коли опрацьовують персональні дані з метою задоволення суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей. Відповідні умови та гарантії можуть тягти за собою спеціальні процедури, спрямовані на реалізацію прав суб'єктів даних, якщо це є належним у світлі цілей, яких прагнуть досягти в результаті спеціального опрацювання разом з технічними та організаційними інструментами, спрямованими на мінімізацію опрацювання персональних даних відповідно до принципів пропорційності та необхідності. Опрацювання персональних даних для наукових цілей необхідно також здійснювати з дотриманням іншого відповідного законодавства, наприклад, законодавства про клінічні випробування.

157. Об'єднуючи інформацію з реєстрів, дослідники можуть отримати нові знання важливого значення щодо таких поширених медичних станів, як серцево-судинне захворювання, рак чи депресія. На підставі реєстрів можна підсилити результати досліджень, оскільки вони охоплюють більшу кількість населення. У суспільних науках дослідження на підставі реєстрів дають можливість отримати необхідні знання про тривалі взаємозв'язки таких суспільних явищ, як безробіття та освіта, їх залежність від життєвих умов. Використання реєстрів дає змогу отримати міцні високоякісні знання, що можуть становити основу для модернізації політики, заснованої на знаннях, поліпшити якість життя значної кількості людей, підвищити ефективність надання соціальних послуг. Опрацьовуючи персональні дані для цілей наукового дослідження, необхідно дотримуватися відповідних умов і гарантій, встановлених законодавством Союзу чи держави-члена.

158. Опрацьовуючи персональні дані для архівних цілей, треба враховувати, що цей Регламент не застосовують до померлих осіб. Публічними органами або публічними чи приватними органами, що ведуть суспільно корисні записи, повинні виступати служби, що, згідно з законодавством Союзу чи держави-члена, мають право отримувати, зберігати, оцінювати, проводити, описувати, повідомляти, сприяти веденню, розповсюджувати та надавати доступ до записів тривалого значення в інтересах суспільства. Держави-члени повинні також мати повноваження на подальше опрацювання персональних даних для цілей архівації, наприклад, для надання спеціальної інформації, що стосується політичної поведінки за умов колишніх режимів тоталітарних держав, геноциду, злочинів проти людяності, зокрема, Голокосту, або воєнних злочинів.

159. Цей Регламент також поширюється на опрацювання персональних даних для цілей наукових досліджень. У межах цього Регламенту опрацювання персональних даних для цілей наукового дослідження необхідно тлумачити в широкому сенсі, у тому числі, наприклад, в аспекті технологічних розробок і демонстрації, фундаментальних досліджень, прикладного дослідження і дослідження за фінансової підтримки з боку приватного сектора. Крім того, необхідно враховувати мету Союзу, відображену в ст. 179 (1) ДФЄС щодо формування Європейського дослідницького простору. Цілі наукового дослідження також включають навчання для задоволення суспільних потреб у сфері охорони здоров'я. Опрацювання персональних даних для цілей наукового дослідження має свої особливості і тому вимагає застосування спеціальних умов, зокрема, в тому, що стосується опублікування чи іншого розкриття персональних даних у контексті цілей наукового дослідження. Якщо результати наукового дослідження, зокрема в контексті здоров'я, дають підстави для вжиття подальших заходів в інтересах суб'єкта даних, необхідно застосувати загальні норми цього Регламенту.

160. Цей Регламент також поширюється на опрацювання персональних даних для цілей історичних досліджень. У процесі історичних досліджень, зокрема досліджень для генеалогічних цілей, цей Регламент не застосовують до померлих осіб.

161. Для цілі надання згоди на участь у науково-дослідницькій діяльності в ході клінічних випробувань необхідно застосовувати відповідні положення Регламенту Європейського Парламенту і Ради (ЄС) № 536/2014*.

162. Цей Регламент також поширюється на опрацювання персональних даних для статистичних цілей. У законодавстві Союзу чи держави-члена необхідно, згідно з Регламентом, передбачити контроль за доступом, особливості опрацювання персональних даних для статистичних цілей, відповідні заходи для захисту прав і свобод суб'єкта даних та забезпечення статистичної конфіденційності. Статистичним цілям підпорядкована будь-яка операція щодо збирання та опрацювання персональних даних, необхідних для статистичних спостережень або для підготування статистичних звітів. Такі статистичні звіти можуть надалі використовуватися для різних цілей, у тому числі для цілей наукового дослідження. Статистична ціль передбачає, що результат опрацювання для статистичних цілей є не персональними даними, а агрегованими даними, та що цей результат або персональні дані не використовують задля підтримки заходів або рішень щодо будь-якої визначеної фізичної особи.

163. Будь-яка конфіденційна інформація, яку Союз і національні органи статистики збирають для підготування офіційної європейської та офіційної національної статистики, має бути захищена. Європейську

* Регламент Європейського Парламенту і Ради (ЄС) № 536/2014 від 16 квітня 2014 р. про клінічні випробування лікарських препаратів, призначених для використання людиною, та скасування Директиви 2001/20/ЄС (OB L 158, 27.05.2014, с. 1).

статистику необхідно розробляти, готувати та розповсюджувати згідно зі статистичними принципами, викладеними в ст. 338 (2) ДФЄС, а національну статистику також – відповідно до законодавства держави-члена. Регламент Європейського Парламенту і Ради (ЄС) № 223/2009* містить вимоги до статистичної конфіденційності для європейської статистики.

164. Щодо повноважень наглядових органів отримувати від контролера або оператора доступ до персональних даних і доступ до їхніх приміщень держава-член може ухвалити на законодавчому рівні, в межах цього Регламенту, спеціальні норми, окресливши в них професійні обов'язки чи інші рівноцінні обов'язки щодо конфіденційності як заходи, необхідні для узгодження права на захист персональних даних із обов'язком збереження професійної таємниці. Це не обмежує чинних зобов'язань держави-члена ухвалювати норми щодо професійної таємниці, якщо цього вимагає за законодавство Союзу.

165. Цей Регламент поважає та не обмежує статус церков і релігійних громад чи спільнот, затверджений чинним конституційним правом держав-членів, як це визнано у ст. 17 ДФЄС.

166. Для виконання цілей цього Регламенту, а саме, для захисту фундаментальних прав і свобод фізичних осіб і, зокрема, їхнього права на захист персональних даних, а також для забезпечення вільного переміщення персональних даних у межах Союзу Комісії необхідно делегувати повноваження на ухвалення актів, згідно зі ст. 290 ДФЄС. Зокрема, делеговані акти необхідно ухвалювати з урахуванням критеріїв і вимог до механізмів сертифікації, інформацію необхідно подавати у форматі стандартизованих іконок і процедур. Особливо важливими є консультації, які проводить Комісія під час своєї підготовчої роботи, в тому числі на рівні експертів. Комісія, під час підготування та розроблення делегованих актів, повинна забезпечувати одночасне, своєвчасне та належне передавання відповідних документів до Європейського Парламенту і Ради.

167. Для забезпечення єдиних умов імплементації цього Регламенту Комісії необхідно надати виконавчі повноваження, якщо це передбачено Регламентом. Реалізацію таких повноважень необхідно здійснювати відповідно до Регламенту (ЄС) № 182/2011. У такому контексті Комісія повинна розглянути спеціальні інструменти для мікропідприємств, малих і середніх підприємств.

168. Експертну процедуру необхідно застосовувати при ухваленні імплементаційних актів щодо стандартних договірних положень між кон-

---

* Регламент Європейського Парламенту і Ради (ЄС) № 223/2009 від 11 березня 2009 р. про європейську статистику та про скасування Регламенту Європейського Парламенту і Ради (ЄС, Євратом) № 1101/2008 про передавання конфіденційних статистичних даних до Статистичного управління Європейських Співтовариств, Регламенту Ради (ЄС) № 322/97 про статистику Співтовариства, та Рішення Ради 89/382/ЄЕС, Євратом, про створення Комітету статистичної програми Європейських Співтовариств (OB L 87, 31.03.2009, с. 164).

тролерами і операторами та між операторами; кодексів поведінки; технічних стандартів і механізмів сертифікації; належного рівня захисту, який надають третя країна, територія чи спеціальний сектор у межах третьої країни, або міжнародна організація; стандартних положень про захист; форматів і процедур обміну інформацією електронними засобами між контролерами, операторами та наглядовими органами щодо зобов'язальних корпоративних правил; взаємної допомоги; домовленостей про обмін інформацією електронними засобами між наглядовими органами та між наглядовими органами і Радою.

169. Якщо є докази того, що третя країна, територія чи спеціальний сектор у межах такої третьої країни, або міжнародна організація не забезпечують належного рівня захисту, Комісія повинна негайно ухвалити застосовні імплементаційні акти.

170. Оскільки мети цього Регламенту, зокрема щодо забезпечення належного рівня захисту фізичних осіб і вільного переміщення персональних даних у всьому Союзі, не можна досягти достатньою мірою на рівні держав-членів, але, з огляду на масштаб запропонованої ініціативи, її можна досягти на рівні Союзу, Союз може ухвалити інструменти, спираючись на принцип субсидіарності, як це передбачено ст. 5 Договору про Європейський Союз. Відповідно до принципу пропорційності, викладеного у цій статті, цей Регламент не виходить за межі необхідного для досягнення такої цілі.

171. Регламент скасовує Директиву 95/46/ЄС. Опрацювання, що вже розпочато станом на дату набуття чинності цим Регламентом, необхідно узгодити з цим Регламентом протягом двох років. Якщо опрацювання засновано на згоді, відповідно до Директиви 95/46/ЄС, суб'єкт даних не має потреби надавати повторну згоду, якщо спосіб, у який надано згоду, відповідає умовам цього Регламенту і, отже, дозволяє контролеру продовжувати таке опрацювання після дати набуття чинності цим Регламентом. Ухвалені Комісією рішення та дозволи, надані наглядовими органами на підставі Директиви 95/46/ЄС, залишаються чинними, поки їх не буде змінено, замінено або скасовано.

172. З Європейським інспектором із захисту даних проведено консультацію згідно зі ст. 28 (2) Регламенту (ЄС) № 45/2001, він надав висновок 7 березня 2012 р.*.

173. Цей Регламент поширюється на всі питання, що стосуються захисту фундаментальних прав і свобод у зв'язку з опрацюванням персональних даних, що не є предметом конкретних зобов'язань з тією самою метою, яку визначено в Директиві Європейського Парламенту і Ради 2002/58/ЄС**, у тому числі зобов'язань, покладених на контролера, і прав

* OB C 192, 30.06.2012, c. 7.

** Директива Європейського Парламенту і Ради 2002/58/ЄС від 12 липня 2002 р. щодо опрацювання персональних даних і захисту приватності в секторі електронних комунікацій (Директива про приватність та електронні комунікації) (OB L 201, 31.07.2002, c. 37).

фізичних осіб. Щоб роз'яснити взаємозв'язок між цим Регламентом і Директивою 2002/58/ЄС, необхідно внести відповідні зміни та доповнення до зазначеної Директиви. Після ухвалення цього Регламенту Директиву 2002/58/ЄС необхідно переглянути, зокрема, з метою забезпечення її відповідності Регламенту,

ухвалили цей Регламент <...>*

* Повний текст див. за посиланням http://medicallaw.org.ua/fileadmin/user_upload/pdf/22_reglament.pdf