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,

---

* Офіційний переклад, текст відредагований.

Беручи до уваги висновок Європейського економічно-соціального комітету*,

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

---

* ОВ С 229, 31.07.2012, с. 90.

** 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).

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, 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 фундаментальних 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 мікропідприємтв, 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

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

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, розпочатої 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

---

* 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).

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

---

* 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).

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, 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.

---

* 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).

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 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 опрацьовує 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 гене-

тичних 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.

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.

---

* 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).

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 особ-

ливий 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 сформульо-

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

вану 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 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

---

* 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 (ОВ L 354, 31.12.2008, с. 70).

партіями персональних даних про політичні переконання населення. Дозвіл на опрацювання таких даних можна надавати з урахуванням суспільного інтересу, за умови впровадження відповідних заходів безпеки.

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 виняткова 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 сформульовавною, 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 інформа-

цію 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 забезпечувати 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, виняткова 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 пове-

дінки 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 елементом 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 і 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 між-

* 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).

народну 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 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 про-

вадяться 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 опрацю-

ванням 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'язального 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 забезпе-

чити 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.

148. З метою розширення сфери застосування норм цього Регламенту, санкції, в тому числі адміністративні штрафи,

* 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 (ОВ L 351, 20.12.2012, с. 1).

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 та відступи, 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 персональних 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

* 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).

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 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 офі-

* 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 (ОВ L 158, 27.05.2014, с. 1).

ційної європейської та офіційної національної статистики, має бути захищена. Європейську 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

---

* 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 (ОВ L 87, 31.03.2009, с. 164).

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 контролерами 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 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,

---

* ОВ С 192, 30.06.2012, с. 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) (ОВ L 201, 31.07.2002, с. 37).

УХВАЛИЛИ ЦЕЙ РЕГЛАМЕНТ:

Розділ I. Загальні положення

Стаття 1

Предмет і цілі

1. Регламент установлює норми щодо захисту фізичних осіб у зв'язку з опрацюванням персональних даних і норми про вільне переміщення персональних даних.

2. Регламент захищає фундаментальні права і свободи фізичних осіб, зокрема їхнє право на захист персональних даних.

3. Вільне переміщення персональних даних у всьому Союзі не повинно бути обмежене чи заборонене з причин, пов'язаних із захистом фізичних осіб у зв'язку з опрацюванням персональних даних.

Стаття 2

Матеріальна сфера дії

1. Регламент поширюється на опрацювання персональних даних повністю чи частково із застосуванням автоматизованих засобів і на опрацювання персональних даних із застосуванням неавтоматизованих засобів, які формують частину картотеки або призначені для внесення до картотеки.

2. Регламент не застосовують до опрацювання персональних даних:

a) у діяльності, що виходить за межі дії права Союзу;

b) держави-члени в діяльності, що виходить за межі глави 2 розділу V Договору про ЄС;

c) фізичні особи для задоволення особистих чи побутових потреб;

d) компетентні органи для цілей запобігання, розслідування, виявлення або переслідування за вчинення кримінальних злочинів або для виконання кримінальних покарань, у тому числі для захисту від загроз громадській безпеці або запобігання таким загрозам.

3. До опрацювання персональних даних установами, органами, службами та агенціями Союзу застосовують Регламент

(ЄС) № 45/2001. Регламент (ЄС) № 45/2001 та інші нормативно-правові акти Союзу, застосовні до такого опрацювання персональних даних, необхідно адаптувати до принципів і правил цього Регламенту, відповідно до ст. 98.

4. Регламент не перешкоджає застосуванню Директиви 2000/31/ЄС, зокрема, норм щодо відповідальності надавачів послуг, передбачених ст. 12–15 зазначеної Директиви.

Стаття 3

Територіальна сфера дії

1. Чинність Регламенту поширюється на опрацювання персональних даних у контексті діяльності осідку контролера або оператора в Союзі, незалежно від того, чи відбувається саме опрацювання в межах Союзу.

2. Чинність Регламенту поширюється на опрацювання персональних даних суб'єктів даних, які перебувають у Союзі, контролером або оператором з осідком поза межами Союзу, якщо опрацювання даних пов'язане з:

a) постачанням товарів чи наданням послуг таким суб'єктам даних у Союзі, незалежно від того, чи вимагають оплату від таких суб'єктів даних;

b) моніторингом поведінки суб'єктів даних у межах Союзу.

3. Чинність Регламенту поширюється на опрацювання персональних даних контролером з осідком поза межами Союзу, але в місці, де чинне законодавство держави-члена як складова публічного міжнародного права.

Стаття 4

Терміни та означення

Для цілей цього Регламенту:

1) «персональні дані» – будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, – особа, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами, як ім'я, ідентифікаційний номер, відомості про місце перебування, онлайн-ідентифікатор, або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної,

генетичної, розумової, економічної, культурної чи соціальної сутності цієї фізичної особи;

2) «опрацювання» – будь-яка операція або низка операцій над персональними даними або наборами персональних даних з використанням таких автоматизованих засобів, як збирання, реєстрація, організація, структурування, зберігання, адаптація чи зміна, пошук, ознайомлення, використання, розкриття через передавання, розповсюдження чи надання іншим чином, упорядкування чи комбінування, обмеження, стирання чи знищення, або без них;

3) «обмеження опрацювання» – позначення збережених персональних даних з метою обмеження їх опрацювання в майбутньому;

4) «профайлінг» – будь-яка форма автоматизованого опрацювання персональних даних, що полягає у використанні персональних даних для оцінювання окремих персональних аспектів, які стосуються фізичної особи, зокрема, для аналізу або прогнозування аспектів, що стосуються продуктивності праці суб'єкта, матеріального становища, здоров'я, особистих здібностей, інтересів, надійності, поведінки, місцезнаходження або пересування;

5) «використання псевдонімів» – опрацювання персональних даних у спосіб, який унеможливлює в подальшому віднесення персональних даних до конкретного суб'єкта даних без використання додаткової інформації, за умови, що таку додаткову інформацію зберігають окремо і на неї поширюється застосування технічних і організаційних інструментів для забезпечення того, щоб персональні дані не були віднесені до фізичної особи, яку ідентифіковано чи можна ідентифікувати;

6) «картотека» – будь-який структурований набір персональних даних, доступ якого надають на підставі до спеціальних критеріїв, може бути централізованим, децентралізованим або розосередженим на функціональній або географічній основі;

7) «контролер» – фізична або юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання

персональних даних; якщо цілі та засоби такого опрацювання визначаються законодавством Союзу чи держави-члена, контролер або спеціальні критерії його призначення можуть бути передбачені законодавством Союзу чи держави-члена;

8) «оператор» – фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який опрацьовує персональні дані від імені контролера;

9) «одержувач» – фізична чи юридична особа, орган публічної влади, агентство чи інший орган, якому розкривають персональні дані, незалежно від того, чи є вони третьою стороною. Органи публічної влади, які можуть отримувати персональні дані в межах конкретного запиту, згідно з законодавством Союзу чи держави-члена, не є одержувачами; опрацювання таких даних органами публічної влади повинно відповідати застосовним нормам про захист даних з урахуванням цілей опрацювання;

10) «третя сторона» – фізична чи юридична особа, орган публічної влади, агентство чи орган, який не є суб'єктом даних, контролером, оператором та особами, які, під безпосереднім керівництвом контролера або оператора, уповноважені опрацьовувати персональні дані;

11) «згода» суб'єкта даних – будь-яке вільно надане, конкретне, поінформоване та однозначне виявлення бажання суб'єкта даних, яким він або вона, шляхом оформлення заяви чи чіткими ствердними діями, підтверджує згоду на опрацювання своїх персональних даних;

12) «порушення захисту персональних даних» – порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, які передано, збережено або іншим чином опрацьовано;

13) «генетичні дані» – персональні дані, що стосуються вроджених або набутих генетичних ознак фізичної особи і містять унікальну інформацію про фізіологію чи здоров'я такої фізичної особи та такі, що отримані, зокрема, в результаті аналізу біологічної проби, взятої у відповідної фізичної особи;

14) «біометричні дані» – персональні дані, отримані внаслідок спеціального технічного опрацювання, що стосується таких фізичних, фізіологічних чи поведінкових ознак фізичної особи, як зображення обличчя чи дактилоскопічні дані, і дають змогу однозначно ідентифікувати фізичну особу або підтверджують її однозначну ідентифікацію;

15) «дані стосовно стану здоров'я» – персональні дані, що стосуються стану фізичного чи психічного здоров'я фізичної особи, в тому числі надання медичних послуг, які відображають інформацію про її стан здоров'я;

16) «головний осідок»:

a) щодо контролера, який має осідки в декількох державах-членах, – осідок його центральної адміністрації в Союзі, за винятком випадків, коли рішення про цілі та засоби опрацювання персональних даних ухвалено в іншому осідку контролера в Союзі і якщо такий інший осідок має повноваження забезпечувати виконання таких рішень; у такому разі осідок, де було ухвалено рішення, вважається головним;

b) щодо оператора, який має осідки в декількох державах-членах, – осідок його центральної адміністрації в Союзі, або, якщо оператор не має центральної адміністрації в Союзі, осідок оператора в Союзі, де відбувається основне опрацювання даних у контексті діяльності осідку оператора тією мірою, якою на оператора поширюються конкретні обов'язки, згідно з цим Регламентом;

17) «представник» – фізична чи юридична особа, що перебуває чи має осідок у Союзі, призначена контролером або оператором розпорядженням у письмовій формі, згідно зі ст. 27, представляє контролера або оператора у питаннях, що стосуються їхніх обов'язків, окреслених цим Регламентом;

18) «підприємство» – фізична чи юридична особа, що провадить господарську діяльність, незалежно від організаційно-правової форми; в тому числі партнерства чи асоціації, що провадять господарську діяльність на постійній основі;

19) «група підприємств» – і підприємство, яке контролює, і підприємства, які перебувають під його контролем;

20) «зобов'язальні корпоративні правила» – політика захисту персональних даних, якої дотримується контролер або оператор, що має осідок на території держави-члена, для здійснення передавання або низки актів передавання персональних даних контролеру або оператору в одній або декількох третіх країнах у межах групи підприємств, або групи підприємств, що провадять спільну господарську діяльність;

21) «наглядовий орган» – незалежний публічний орган, створений державою-членом відповідно до ст. 51;

22) «відповідний наглядовий орган» – наглядовий орган, якого стосується опрацювання персональних даних, оскільки:

a) контролер або оператор має осідок на території держави-члена такого наглядового органу;

b) суб'єкти даних, що перебувають на території держави-члена такого наглядового органу, зазнають істотного впливу чи ймовірно зазнаватимуть істотного впливу внаслідок опрацювання;

c) до такого наглядового органу подано скаргу;

23) «транскордонне опрацювання»:

a) опрацювання персональних даних, що відбувається у контексті діяльності осідків контролера чи оператора в Союзі більше ніж в одній державі-члені, якщо контролер або оператор мають осідки більше ніж в одній державі-члені;

b) опрацювання персональних даних, що відбувається у контексті діяльності єдиного осідку контролера або оператора в Союзі, але істотно впливає чи ймовірно істотно впливатиме на суб'єктів даних у декількох державах-членах;

24) «відповідне і вмотивоване заперечення» – заперечення проти проекту рішення щодо того, чи має місце порушення цього Регламенту, чи відповідають цьому Регламенту передбачені заходи щодо контролера або оператора, що чітко вказують на значущість ризиків, які спричиняє проект рішення, для фундаментальних прав і свобод суб'єктів даних та, у відповідних випадках, вільного переміщення персональних даних у межах Союзу;

25) «послуга інформаційного суспільства» – послуга, як її означено в пп. *b* ст. 1 (1) Директиви Європейського Парламенту і Ради (ЄС) 2015/1535*;

26) «міжнародна організація» – організація та підпорядковані їй органи, діяльність яких регулюється публічним міжнародним правом, або будь-який інший орган, заснований договором або на підставі договору між двома чи декількома державами.

Розділ II. Принципи

Стаття 5

Принципи опрацювання персональних даних

1. Персональні дані необхідно:

a) опрацьовувати у законний, правомірний і прозорий спосіб щодо суб'єкта даних

«законність, правомірність і прозорість»);

b) збирати для визначених, чітких і законних цілей і в подальшому не опрацьовувати у спосіб, що суперечить таким цілям; подальше опрацювання для задоволення суспільних інтересів чи цілей наукового або історичного дослідження, статистичних цілей не можна вважати, згідно зі ст. 89 (1), несумісним з первинними цілями («цільове обмеження»);

c) вважати достатніми і відповідними та обмежити їх ступенем необхідності з огляду на цілі опрацювання («мінімізація даних»);

d) вважати точними і, за необхідності, оновлювати; необхідно вживати усіх відповідних заходів для того, щоб неточні персональні дані, зважаючи на цілі їх опрацювання, були вилучені або виправлені без затримки («точність»);

e) зберігати в формі, що уможливлює ідентифікацію суб'єктів даних не довше, ніж це необхідно для цілей опрацювання; персональні дані можна зберігати протягом більш тривалих

---

* Директива Європейського Парламенту і Ради 2015/1535/ЄС від 9 вересня 2015 р. про порядок надання інформації у сфері технічних регламентів і правила щодо послуг інформаційного суспільства (ОВ L 241, 17.09.2015, с. 1).

періодів, доки їх опрацьовують винятково для досягнення суспільно корисних цілей, цілей наукового чи історичного дослідження, статистичних цілей, відповідно до ст. 89 (1), за умов вжиття відповідних технічних і організаційних заходів, передбачених цим Регламентом для гарантування прав і свобод суб'єкта даних («обмеження зберігання»);

f) опрацьовувати в спосіб, що забезпечує належну безпеку персональних даних, у тому числі захист від несанкціонованого чи незаконного опрацювання та від ненавмисної втрати, знищення чи заподіяння шкоди, із застосуванням відповідних технічних і організаційних інструментів («цілісність і конфіденційність»).

2. Контролер несе відповідальність за дотримання параграфа 1 і повинен бути здатним це довести («підзвітність»).

Стаття 6

Законність опрацювання

1. Опрацювання є законним, лише якщо виконано та мірою виконання принаймні однієї з наведених нижче умов:

a) суб'єкт даних надав згоду на опрацювання своїх персональних даних для однієї чи декількох спеціальних цілей;

b) опрацювання є необхідним для виконання контракту, стороною якого є суб'єкт даних, або для вчинення дій на запит суб'єкта даних до укладення договору;

c) опрацювання є необхідним для дотримання встановленого законом зобов'язання, яке поширюється на контролера;

d) опрацювання є необхідним для того, щоб захистити життєво важливі інтереси суб'єкта даних або іншої фізичної особи;

e) опрацювання є необхідним для виконання суспільно корисного завдання або здійснення офіційних повноважень, покладених на контролера;

f) опрацювання є необхідним для задоволення законних інтересів контролера або третьої сторони, окрім випадків, коли над такими інтересами переважають інтереси фундаментальних прав і свобод суб'єкта даних, що вимагають охорони персональних даних, особливо, якщо суб'єктом даних є дитина.

Підпункт *f* п. 1 не стосується опрацювання, яке здійснюють публічні органи, виконуючи свої завдання.

2. Держави-члени можуть мати або запроваджувати уточнені положення до норм цього Регламенту щодо опрацювання з метою дотримання пп. *c* і *e* п. 1, більш чітко окреслюючи спеціальні вимоги до опрацювання та інші засоби забезпечення законного та правомірного опрацювання, в тому числі щодо інших спеціальних ситуацій опрацювання, як це передбачено розділом IX.

3. До законодавчої бази, вказаної в пп. *c* і *e* п. 1, належать:

a) законодавство Союзу; або

b) законодавство держави-члена, яке поширюється на контролера.

Мету опрацювання необхідно означити в такій законодавчій базі або, в частині опрацювання, вказаного в пп. *e* п. 1, її необхідно обов'язково передбачити для виконання суспільно корисних завдань чи здійснення офіційних повноважень, покладених на контролера. Така законодавча база може містити спеціальні положення для адаптації застосування правил цього Регламенту, серед інших: загальні умови, що регулюють питання законності опрацювання контролером; типи даних, що підлягають опрацюванню; відповідні суб'єкти даних; установи, яким можна розкривати персональні дані та цілі такого розкриття; цільове обмеження; періоди зберігання; операції опрацювання і процедури опрацювання, в тому числі заходи, спрямовані на забезпечення законного та справедливого опрацювання, такі як ті, яких вживають в інших спеціальних ситуаціях опрацювання, згідно з розділом IX. Законодавство Союзу або держави-члена повинно відповідати суспільним інтересам і бути пропорційним законній цілі.

4. Якщо опрацювання для іншої цілі ніж та, для якої було зібрано персональні дані, не засноване на згоді суб'єкта даних або на законодавстві Союзу чи держави-члена, що є необхідним і пропорційним заходом у демократичному суспільстві для гарантування цілей, окреслених у ст. 23 (1), контролер, щоб переконатися, чи опрацювання для іншої цілі сумісне із ціллю первинного збирання персональних даних, повинен врахувати, серед іншого:

a) будь-який зв'язок між цілями, для яких збирають персональні дані, і цілями запланованого подальшого опрацювання;

b) контекст збирання персональних даних, зокрема, щодо взаємозв'язку між суб'єктами даних і контролером;

c) специфіку персональних даних, зокрема, питання опрацювання спеціальних категорій персональних даних, згідно зі ст. 9, або опрацювання персональних даних про судимості і кримінальні злочини, згідно зі ст. 10;

d) можливі наслідки запланованого подальшого опрацювання для суб'єктів даних;

e) наявність належних гарантій, що можуть передбачати шифрування чи використання псевдонімів.

Стаття 7

Умови надання згоди

1. Якщо опрацювання засновано на згоді, контролер повинен бути спроможним довести те, що суб'єкт даних надав згоду на опрацювання своїх персональних даних.

2. Якщо суб'єкт даних надає згоду в контексті письмової декларації, що також стосується інших питань, запит на надання згоди необхідно подавати у зрозумілій і доступній формі, що чітко відрізняє її від інших питань, з використанням чітких і простих формулювань. Будь-яка частина такої декларації, що становить порушення цього Регламенту, не є зобов'язальною.

3. Суб'єкт даних повинен мати право відкликати свою згоду в будь-який час. Відкликання згоди не повинно впливати на законність опрацювання, що ґрунтувалося на згоді до її відкликання. Суб'єкта даних необхідно про це повідомити перед наданням згоди. Необхідно забезпечити однакову можливість як для відкликання, так і для надання згоди.

4. Оцінюючи те, чи згода надана добровільно, необхідно врахувати те, чи залежить, окрім іншого, виконання договору, в тому числі надання послуги, від згоди на опрацювання персональних даних, необхідної для виконання такого договору.

Стаття 8

Умови, застосовні до згоди дитини в сфері послуг інформаційного суспільства

1. У разі застосування пп. *a* ст. 6 (1) у сфері пропозиції послуг інформаційного суспільства безпосередньо дитині опрацювання персональних даних дитини є законним якщо дитина досягла щонайменше 16 років. Якщо дитина не досягла 16 років, таке опрацювання є законним, лише за умови, що згоду надано чи її надання санкціоновано носієм батьківської відповідальності щодо дитини.

Держави-члени можуть передбачити в законі нижчий вік для таких цілей за умови, що цей вік не нижчий за 13 років.

2. Контролер повинен докласти розумних зусиль для перевірки в таких випадках того, що згоду надано чи її надання санкціоновано носієм батьківської відповідальності щодо дитини.

3. Пункт 1 не впливає на загальне договірне право держав-членів, зокрема на правила щодо законності укладення чи наслідків контракту для дитини.

Стаття 9

Опрацювання спеціальних категорій персональних даних

1. Заборонено опрацювання персональних даних, що розкривають расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, членство в професійних спілках, а також опрацювання генетичних даних, біометричних даних для цілі єдиної ідентифікації фізичної особи, даних стосовно стану здоров'я чи даних про статеве життя фізичної особи чи її сексуальної орієнтації.

2. Пункт 1 не застосовують, якщо застосовують таке:

a) суб'єкт даних надав явну згоду на опрацювання таких персональних даних для однієї чи декількох визначених цілей, за винятком випадків, якщо законодавством Союзу чи держави-члена передбачено, що суб'єкт даних не може зняти заборону, вказану в п. 1;

b) опрацювання необхідне для цілей виконання обов'язків і здійснення спеціальних прав контролера або суб'єкта даних

у сфері зайнятості та права соціального забезпечення і соціального захисту, якщо воно дозволено законодавством Союзу або держави-члена чи колективною угодою, укладеною згідно з законодавством держави-члена, що надає необхідні гарантії для захисту фундаментальних прав та інтересів суб'єкта даних;

c) опрацювання необхідне для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи, якщо суб'єкт даних фізично чи юридично неспроможний надати згоду;

d) опрацювання здійснюють у ході відповідної законної діяльності з необхідними гарантіями установою, асоціацією чи будь-яким іншим некомерційним органом з політичною, філософською, релігійною ціллю або для цілі професійної спілки та за умови, що опрацювання стосується виняткового членів чи колишніх членів органу або осіб, які підтримують регулярні контакти з ними у зв'язку з його цілями, та що персональні дані не розкривають поза межами такого органу без згоди суб'єктів даних;

e) опрацювання стосується персональних даних, що відкрито оприлюднені суб'єктом даних;

f) опрацювання необхідне для формування, здійснення або захисту правових претензій або якщо суди діють як судові органи;

g) опрацювання необхідне з причин суттєвого суспільного інтересу, на підставі законодавства Союзу або держави-члена, що має бути пропорційним цілі, якої прагнуть досягти, поважати сутність права на захист даних і передбачати належні та спеціальні заходи для захисту фундаментальних прав та інтересів суб'єкта даних;

h) опрацювання необхідне для цілей превентивної медицини чи гігієни праці, для оцінювання працездатності працівника, медичного діагнозу, надання послуг у сфері охорони здоров'я, соціального забезпечення чи лікування або управління системами та послугами в сфері охорони здоров'я, соціального забезпечення чи лікування на підставі законодавства Союзу або держави-члена чи відповідно до контракту з медичним працівником і з урахуванням умов і гарантій, зазначених у п. 3;

i) опрацювання необхідне для задоволення суспільних

інтересів у сфері охорони громадського здоров'я, зокрема, захисту від серйозних транскордонних загроз здоров'ю чи забезпечення високих стандартів якості та безпеки в сфері охорони здоров'я і лікарських препаратів або медичного обладнання, на підставі законодавства Союзу або держави-члена, що передбачає належні та спеціальні заходи для захисту прав і свобод суб'єкта даних, зокрема, професійної таємниці;

j) опрацювання необхідне для досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження або статистичних цілей, відповідно до ст. 89 (1), на підставі законодавства Союзу або держави-члена, що має бути пропорційним цілі, якої прагнуть досягти, поважати сутність права на захист даних і передбачати належні та спеціальні заходи для захисту фундаментальних прав та інтересів суб'єкта даних.

3. Персональні дані, зазначені в п. 1, можна опрацьовувати для цілей, зазначених у пп. *h* п. 2, якщо такі дані опрацьовує фахівець або їх опрацьовують за його відповідальністю з урахуванням обов'язку збереження професійної таємниці, згідно з законодавством Союзу або держави-члена чи нормами, встановленими національними компетентними органами чи іншою особою, також з урахуванням обов'язку збереження таємниці згідно з законодавством Союзу або держави-члена чи нормами, встановленими національними компетентними органами.

4. Держави-члени можуть мати або запроваджувати деталізовані умови, в тому числі обмеження стосовно опрацювання генетичних даних, біометричних даних або даних про стан здоров'я.

Стаття 10

Опрацювання персональних даних про судимості і кримінальні злочини

Опрацювання персональних даних про судимості і кримінальні злочини або пов'язані заходи безпеки на підставі ст. 6 (1) здійснюють лише під контролем офіційного органу або у разі, якщо опрацювання дозволено законодавством Союзу чи держави-члена, що передбачають належні гарантії для прав

і свобод суб'єктів даних. Будь-який всеосяжний реєстр судимостей необхідно вести лише під контролем офіційного органу.

Стаття 11

Опрацювання, що не вимагає ідентифікації

1. 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.

2. Якщо, в ситуаціях, вказаних у п. 1 цієї статті, контролер здатний довести, що не може ідентифікувати суб'єкта даних, він, за можливості, повинен повідомити про це суб'єкта даних. У таких ситуаціях ст. 15–20 не застосовують, окрім винятків, коли суб'єкт даних, з метою реалізації своїх прав за зазначеними статтями, надає додаткову інформацію, що уможливлює його ідентифікацію.

Розділ III. Права суб'єкта даних

Секція 1

Прозорість і форми

Стаття 12

Прозора інформація, повідомлення та форми реалізації прав суб'єкта даних

1. Контролер повинен вжити необхідних заходів для надання будь-якої інформації, вказаної в ст. 13 і 14 і в будь-якому повідомленні, згідно зі ст. 15–22 і 34, щодо опрацювання, суб'єкту даних у стислій, прозорій, доступній для розуміння формі, з використанням чітких і простих формулювань, зокрема, для надання будь-якої інформації, спеціально призначеної для дитини. Інформацію необхідно надавати у письмовій формі або іншій формі, в тому числі, за необхідності, електронній. У разі надання запиту суб'єктом даних інформація може бути усною, за умови, що особу суб'єкта даних встановлено іншими засобами.

2. Контролер повинен сприяти реалізації прав суб'єктом даних, згідно зі ст. 15–22. У випадках, вказаних у ст. 11 (2), контролер не має права ухилятися від дій на запит суб'єкта даних щодо реалізації його прав за ст. 15–22, за винятком випадків, коли контролер спроможний довести неможливість ідентифікації суб'єкта даних.

3. Контролер повинен надати інформацію щодо заходів, вжитих на запит за ст. 15–22, суб'єкту даних без необґрунтованої затримки та в будь-якому випадку протягом одного місяця з дати отримання запиту. За необхідності, враховуючи складність і кількість запитів, цей період можна подовжити на два наступні місяці. Контролер повинен повідомити суб'єкта даних про будь-яке таке подовження протягом одного місяця з дати отримання запиту, а також – про причини затримки. Якщо суб'єкт даних надає запит за допомогою електронних засобів, інформацію, за можливості, необхідно надати електронними засобами, за винятком випадків, коли суб'єкт даних попросить про інше.

4. Якщо контролер не вживає заходів у відповідь на запит суб'єкта даних, він повинен повідомити суб'єкта даних без затримки та щонайменше протягом одного місяця з дати отримання запиту про причини утримання від дій і про можливість подання скарги до наглядового органу та звернення до засобів судового захисту.

5. Надавати інформацію, за ст. 13 і 14, будь-яке повідомлення та вживати будь-яких заходів, за ст. 15–22 і 34, необхідно на безоплатній основі. Якщо запити від суб'єкта даних є явно необґрунтованими чи надмірними, зокрема, через їх багатократне повторення, контролер може або:

a) стягнути розумну плату, враховуючи адміністративні витрати на надання інформації або повідомлення чи вжиття заходів у відповідь на запит; або

b) ухилитися від виконання заходів у відповідь на запит.

На контролера необхідно покласти додаткове зобов'язання щодо доведення явно необґрунтованого чи надмірного характеру запиту.

6. Без обмеження ст. 11, якщо контролер має вагомі підстави сумніватися в особистості фізичної особи, яка подала

запит, вказаний у ст. 15–21, контролер може надіслати запит про надання додаткової інформації, необхідної для підтвердження особистості суб'єкта даних.

7. Інформацію, яку необхідно надати суб'єктам даних, відповідно до ст. 13 і 14, можна надавати в поєднанні зі стандартизованими іконками для того, щоб наочно, у доступній для розуміння та чіткій формі показати призначене опрацювання. Іконки, подані в електронній формі, повинні легко зчитуватися машиною.

8. Комісії необхідно надати повноваження ухвалювати делеговані акти згідно зі ст. 92, з метою визначення інформації, яка має бути представлена в іконках, та процедур надання стандартизованих іконок.

Секція 2

Інформація та доступ до персональних даних

Стаття 13

Інформація, яку необхідно надати у разі збирання персональних даних від суб'єкта даних

1. Якщо персональні дані щодо суб'єкта даних отримують від суб'єкта даних, контролер повинен, у момент отримання персональних даних, надати суб'єкту даних усю інформацію, а саме про:

a) особу та контактні дані контролера та, за необхідності, представника контролера;

b) контактні дані співробітника з питань захисту даних, за необхідності;

c) цілі опрацювання, для досягнення яких призначено персональні дані, а також законодавчу базу для опрацювання;

d) якщо опрацювання здійснюють на підставі пп. *f* ст. 6 (1), законні інтереси контролера або третьої сторони;

e) одержувачів чи категорії одержувачів персональних даних, за наявності;

f) за необхідності, інформацію про те, що контролер має намір передати персональні дані до третьої країни чи міжнародної організації, про наявність чи відсутність рішення

Комісії про відповідність, або, у випадку актів передавання, вказаних у ст. 46 чи 47, або пп. 2 ст. 49 (1), – повідомити про належні чи відповідні гарантії та засоби, за допомогою яких можна отримати копію таких даних, або про джерела, де вони є у вільному доступі.

2. Крім інформації, вказаної в п. 1, контролер повинен, у момент отримання персональних даних, надати суб'єкту даних усю детальну інформацію, необхідну для забезпечення правомірного та прозорого опрацювання, а саме інформацію про:

a) період зберігання персональних даних, або, якщо це неможливо, – критерії визначення такого періоду;

b) існування права на запит від контролера щодо доступу до персональних даних і їх виправлення, вилучення, обмеження опрацювання щодо суб'єкта даних або на заперечення проти опрацювання, а також права на мобільність даних;

c) якщо опрацювання здійснюють на підставі пп. *a* ст. 6 (1) або пп. *a* ст. 9 (2), – існування права на відкликання згоди в будь-який момент, без наслідків для законності опрацювання, заснованого на згоді, наданій перед її відкликанням;

d) право подавати скаргу до наглядового органу;

e) те, чи є надання персональних даних статутною, договірною вимогою або вимогою, необхідною для укладення контракту, а також – чи зобов'язаний суб'єкт даних надати персональні дані, та про можливі наслідки ненадання таких даних;

f) наявність автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу, вказаного в ст. 22 (1) та (4) і, принаймні, в таких випадках, достовірної інформації про логіку, значущість і передбачувані наслідки такого опрацювання для суб'єкта даних.

3. Якщо контролер має намір надалі опрацьовувати персональні дані для іншої цілі ніж та, для якої персональні дані було отримано, контролер повинен надати суб'єкту даних перед початком подальшого опрацювання інформацію про таку іншу ціль і будь-яку належну детальну інформацію, як вказано в п. 2.

4. Пункти 1, 2 і 3 не застосовують, якщо та оскільки суб'єкт даних уже володіє інформацією.

Стаття 14

Інформація, яку необхідно надати у разі отримання персональних даних не від суб'єкта даних

1. Якщо персональні дані отримано не від суб'єкта даних, контролер повинен надати суб'єкту даних інформацію про:

a) особу та контактні дані контролера та, за необхідності, представника контролера;

b) контактні дані співробітника з питань захисту даних, за необхідності;

c) цілі опрацювання, для досягнення яких призначено персональні дані, а також законодавчу базу для опрацювання;

d) категорії відповідних персональних даних;

e) одержувачів чи категорії одержувачів персональних даних, за наявності;

f) за необхідності, про те, що контролер прагне передати персональні дані до одержувача в третій країні чи міжнародної організації, про наявність чи відсутність рішення Комісії про відповідність, або, у випадку актів передавання, вказаних у ст. 46 чи 47, або пп. 2 ст. 49 (1), – про існування належних чи відповідних гарантій і засобів, за допомогою яких можна отримати копію таких даних, або джерела, де вони є у вільному доступі.

2. Крім інформації, зазначеної в параграфі 1, контролер повинен надати суб'єкту даних інформацію, необхідну для забезпечення правомірного та прозорого опрацювання, що стосується суб'єкта даних, а саме про:

a) період зберігання персональних даних, або, якщо це неможливо, – критерії визначення такого періоду;

b) якщо опрацювання здійснюють на підставі п. *f* ст. 6 (1), законні інтереси контролера або третьої сторони;

c) існування права на запит від контролера щодо доступу до персональних даних і їх виправлення, вилучення, обмеження опрацювання щодо суб'єкта даних і на заперечення опрацювання, а також права на мобільність даних;

d) якщо опрацювання здійснюють на підставі пп. *a* ст. 6 (1) або пп. *a* ст. 9 (2), – існування права на відкликання згоди в будь-який момент, без наслідків для законності опрацювання, що ґрунтувалося на згоді, наданій перед відкликанням;

e) право подавати скаргу до наглядового органу;

f) те, з якого джерела походять персональні дані, та, за необхідності, про те, чи надійшли вони з джерел, доступних для громадськості;

g) наявність автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу, вказаного в ст. 22 (1) та (4) і, принаймні, в таких випадках, достовірної інформації про логіку, значущість і передбачувані наслідки такого опрацювання для суб'єкта даних.

3. Контролер повинен надати інформацію, вказану в п. 1 та 2:

a) у розумний строк після отримання персональних даних, але щонайменше протягом одного місяця, враховуючи конкретні обставини, за яких опрацьовують персональні дані;

b) якщо персональні дані необхідно використати для спілкування з суб'єктом даних, – принаймні в момент першого повідомлення такому суб'єкту даних; або

c) якщо передбачається розкриття іншому одержувачу, – принаймні під час першого розкриття персональних даних.

4. Якщо контролер має намір надалі опрацьовувати персональні дані для іншої цілі ніж та, для якої персональні дані отримано, він повинен надати суб'єкту даних перед початком подальшого опрацювання інформацію про таку іншу ціль і будь-яку належну детальну інформацію, як вказано в п. 2.

5. Пункти 1–4 не застосовують, якщо та оскільки:

a) суб'єкт даних уже володіє інформацією;

b) надання такої інформації стає неможливим чи викликало б несумісні наслідки, зокрема, для опрацювання задля досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей, із урахуванням умов і гарантій, зазначених у ст. 89 (1), або доки обов'язок, вказаний у параграфі 1 цієї статті, ймовірно унеможливить або серйозно обмежить досягнення цілей такого опрацювання. У таких ситуаціях контролер повинен вжити необхідних заходів для захисту прав і свобод та законних інтересів суб'єкта даних, у тому числі оприлюднення інформації;

c) отримання чи розкриття прямо передбачене законодавством Союзу або держави-члена, яке поширюється на контролера та яким передбачено необхідні заходи для захисту законних інтересів суб'єкта даних; або

d) якщо персональні дані необхідно залишати в таємниці відповідно до обов'язку збереження професійної таємниці, що регулюється законодавством Союзу або держави-члена, в тому числі статутного обов'язку збереження таємниці.

Стаття 15

Право суб'єкта даних на доступ

1. Суб'єкт даних повинен мати право на отримання від контролера підтвердження факту опрацювання її або його персональних даних і, якщо це так, – доступ до персональних даних та інформації про:

a) цілі цього Регламенту;

b) категорії відповідних персональних даних;

c) одержувачів чи категорії одержувачів, яким персональні дані були або будуть розкриті, зокрема, одержувачів у третіх країнах або міжнародні організації;

d) за можливості, період, протягом якого передбачається, що персональні дані будуть зберігати, або, якщо це неможливо, – критерії визначення такого періоду;

e) існування права надсилати запит до контролера щодо виправлення чи вилучення персональних даних, або обмеження опрацювання персональних даних про суб'єкта даних і заперечувати проти такого опрацювання;

f) право подавати скаргу до наглядового органу;

g) якщо персональні дані не отримані від суб'єкта даних, будь-яку інформацію щодо їх джерела;

h) наявність автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу, вказаного в ст. 22 (1) та (4) і, принаймні, в таких випадках, достовірної інформації про логіку, значущість і передбачувані наслідки такого опрацювання для суб'єкта даних.

2. Якщо персональні дані передають до третьої країни або до міжнародної організації, суб'єкт даних повинен мати

право бути повідомленим про належні гарантії, відповідно до ст. 46, щодо передавання даних.

3. Контролер повинен надати копію персональних даних, які перебувають у процесі опрацювання. За виготовлення будь-яких подальших копій, запит на які надсилатиме суб'єкт даних, контролер може стягувати розумну плату, що ґрунтується на адміністративних витратах. У разі подання суб'єктом даних запиту електронними засобами і за винятком випадків, коли він просить про іншу форму, інформацію необхідно подавати в загальноприйнятій електронній формі.

4. Право на отримання копії, вказаної в п. 3, не повинно негативно впливати на права та свободи інших осіб.

Секція 3

Виправлення та вилучення

Стаття 16

Право на виправлення

Суб'єкт даних повинен мати право на виправлення його або її неточних персональних даних, яке повинен здійснити контролер без будь-якої необґрунтованої затримки. Зважаючи на цілі опрацювання, суб'єкт даних повинен мати право доповнити неповні персональні дані, в тому числі надавши додаткову заяву.

Стаття 17

Право на вилучення («право бути забутим»)

1. Суб'єкт даних повинен мати право на вилучення своїх персональних даних, яке повинен здійснити контролер без будь-якої безпідставної затримки, також контролер повинен бути зобов'язаним стерти персональні дані без будь-якої необґрунтованої затримки у разі виникнення однієї з таких підстав:

a) немає більше потреби в персональних даних для цілей, для яких їх збирали чи іншим чином опрацьовували;

b) суб'єкт даних відкликає згоду, на якій ґрунтується опрацювання, згідно з п. *a* ст. 6 (1) чи пп. *a* ст. 9 (2), та якщо немає іншої законної підстави для опрацювання;

c) суб'єкт даних заперечує проти опрацювання, згідно зі ст. 21 (1), та немає жодних першорядних законних підстав для опрацювання, або суб'єкт даних заперечує проти опрацювання, згідно зі ст. 21 (2);

d) персональні дані опрацьовували незаконно;

e) персональні дані необхідно вилучити, щоб дотриматися зобов'язання, закріпленого в законодавстві Союзу або держави-члена, яке поширюється на контролера;

f) персональні дані збирали в зв'язку з пропонуванням послуг інформаційного суспільства, вказаних у ст. 8 (1).

2. У разі, якщо контролер оприлюднив персональні дані та є зобов'язаним, відповідно до п. 1, вилучити персональні дані, контролер, з урахуванням можливостей технологій і коштів, призначених для їх реалізації, повинен вжити відповідних заходів, у тому числі технічних, щоб поінформувати контролерів, які опрацьовують персональні дані, про те, що суб'єкт даних надіслав запит про вилучення такими контролерами будь-яких посилань на його персональні дані, їх копій чи відтворень.

3. Пункти 1 та 2 не застосовують (залежно від ступеня необхідності) в опрацюванні:

a) для реалізації права на свободу вияву поглядів і свободу інформації;

b) для дотримання зобов'язання, що вимагає опрацювання, згідно з законодавством Союзу або держави-члена, яке поширюється на контролера, або для виконання суспільно корисних завдань чи офіційних повноважень, покладених на контролера;

c) на підставах суспільного інтересу в сфері охорони громадського здоров'я, згідно з пп. *h* та *i* ст. 9 (2), а також ст. 9 (3);

d) для задоволення суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей, відповідно до ст. 89 (1), мірою, якою вказане в п. 1 ймовірно унеможливить або серйозно обмежить досягнення цілей такого опрацювання;

або

e) для формування, здійснення або захисту правових претензій.

Стаття 18

Право на обмеження опрацювання

1. Суб'єкт даних повинен мати право на обмеження опрацювання контролером за таких обставин:

a) точність персональних даних оскаржує суб'єкт даних, протягом періоду часу, що надає контролеру можливість перевірити точність персональних даних;

b) опрацювання є незаконним і суб'єкт даних виступає проти вилучення персональних даних, а натомість надсилає запит на обмеження їх використання;

c) контролеру більше не потрібні персональні дані для цілей опрацювання, але їх вимагає суб'єкт даних для формування, здійснення або захисту правових претензій;

d) суб'єкт даних заперечив проти опрацювання, згідно зі ст. 21 (1), в очікуванні перевірки щодо того, чи переважають законні підстави контролера над законними інтересами суб'єкта даних.

2. Якщо опрацювання обмежене, відповідно до п. 1, такі персональні дані необхідно, за винятком зберігання, опрацьовувати лише за згоди суб'єкта даних або для подання, реалізації чи захисту правових претензій або для захисту прав іншої фізичної чи юридичної особи чи на підставах важливості суспільного інтересу Союзу або держави-члена.

3. Контролер повинен повідомити суб'єкта даних, який домігся обмеження опрацювання, згідно з параграфом 1, до моменту скасування обмеження на опрацювання.

Стаття 19

Зобов'язання щодо повідомлення про виправлення чи вилучення персональних даних або обмеження опрацювання

Контролер повинен повідомити про будь-яке виправлення чи вилучення персональних даних або обмеження опрацювання, що здійснюють згідно зі ст. 16, ст. 17 (1) і ст. 18, кожного одержувача, якому було повідомлено персональні дані, за винятком випадків, коли це неможливо або викликає несумісні наслідки. Контролер повинен повідомити суб'єкта

даних про таких одержувачів, якщо суб'єкт даних надсилає про це запит.

Стаття 20

Право на мобільність даних

1. Суб'єкт даних повинен мати право на отримання його або її персональних даних, які він надав контролеру, в структурованому, загальноприйнятому форматі, що легко зчитується машиною, та мати право на передавання таких даних іншому контролеру без перешкод від контролера, якому було надано персональні дані, якщо:

a) опрацювання ґрунтується на згоді, наданій згідно з пп. *a* ст. 6 (1) чи пп. *a* ст. 9 (2), або на основі договору, згідно з пп. *b* ст. 6 (1); та

b) опрацювання є автоматизованим.

2. Реалізуючи своє право на мобільність даних, згідно з п. 1, суб'єкт даних повинен мати право на передавання персональних даних безпосередньо від одного контролера до іншого, за умови відповідної технічної можливості.

3. Реалізація права, вказаного в п. 1 цієї статті, не повинна обмежувати чинність ст. 17. Це право не застосовується до опрацювання, необхідного для задоволення суспільних інтересів або виконання офіційних повноважень, покладених на контролера.

4. Право, вказане в п. 1, не повинно негативно впливати на права та свободи інших осіб.

Секція 4

Право на заперечення та автоматизоване індивідуальне вироблення й ухвалення рішень

Стаття 21

Право на заперечення

1. Суб'єкт даних повинен мати право заперечувати, на підставах, що пов'язані з його або її конкретною ситуацією, в будь-який час, проти опрацювання його або її персональних даних, яке здійснюють на підставі пп. *e* чи *f* ст. 6 (1), у тому числі проти профайлінгу, що ґрунтується на цих положеннях.

Контролер не повинен більше опрацьовувати персональні дані, за винятком випадків, коли він довів наявність істотних законних підстав для опрацювання, що переважають над інтересами, правами та свободами суб'єкта даних, або для формування, здійснення або захисту правових претензій.

2. У випадку опрацювання персональних даних для цілей прямого маркетингу суб'єкт даних повинен мати право на заперечення проти такого опрацювання персональних даних, у тому числі профайлінгу, тією мірою, якою це стосуються такого прямого маркетингу.

3. Якщо суб'єкт даних заперечує проти опрацювання для цілей прямого маркетингу, персональні дані не можна більше опрацьовувати для таких цілей.

4. Щонайпізніше в момент першого повідомлення суб'єкту даних про право, вказане в п. 1 і 2, необхідно чітко поінформувати суб'єкта даних, подавши цю інформацію зрозуміло та окремо від будь-якої іншої інформації.

5. У контексті користування послугами інформаційного суспільства та незважаючи на Директиву 2002/58/ЄС, суб'єкт даних може реалізовувати своє право на заперечення автоматизованими засобами з використанням технічних специфікацій.

6. Якщо персональні дані опрацьовують для цілей наукового чи історичного дослідження або для статистичних цілей, згідно зі ст. 89 (1), суб'єкт даних, на підставах, що пов'язані з його або її конкретною ситуацією, повинен мати право на заперечення проти опрацювання його або її персональних даних, за винятком, якщо таке опрацювання необхідне для задоволення суспільних інтересів.

Стаття 22

Автоматизоване індивідуальне вироблення й ухвалення рішень, у тому числі профайлінг

1. Суб'єкт даних повинен мати право не підпорядковуватися рішенню, що ґрунтується винятково на автоматизованому опрацюванні, в тому числі профайлінгу, що породжує правові наслідки для нього чи подібним чином істотно впливає на нього.

2. Параграф 1 не застосовують, якщо рішення:

a) є необхідним для укладення чи виконання договору між суб'єктом даних і контролером даних;

b) дозволено законодавством Союзу або держави-члена, яке поширюється на контролера та яким також передбачено відповідні заходи для захисту прав і свобод та законних інтересів суб'єкта даних; або

c) ґрунтується на прямо висловленій згоді.

3. У ситуаціях, вказаних у пп. *a* та *c* п. 2, контролер даних повинен вжити належних заходів для гарантування охорони прав, свобод, законних інтересів суб'єктів даних, принаймні права на втручання з боку контролера, висловлення своєї думки та оскарження рішення.

4. Рішення, вказані в п. 2, не повинні ґрунтуватися на спеціальних категоріях персональних даних, вказаних у ст. 9 (1), за винятком застосування пп. *a* або *g* ст. 9 (2) та відсутності передбачених належних заходів з охорони прав, свобод, законних інтересів суб'єктів даних.

Секція 5

Обмеження

Стаття 23

Обмеження

1. Законодавство Союзу або держави-члена, яке поширюється на контролера або оператора, може обмежувати за допомогою законодавчого інструмента обсяг обов'язків і прав, передбачений ст. 12–22, 34, 5, відповідно до того, наскільки повно його положення відображають права та обов'язки, передбачені в ст. 12–22, якщо таке обмеження зберігає сутність фундаментальних прав і свобод і є необхідним та пропорційним заходом у демократичному суспільстві для забезпечення:

a) національної безпеки;

b) оборони;

c) громадської безпеки;

d) запобігання, розслідування, виявлення або переслідування за скоєння кримінальних злочинів або для виконання

кримінальних покарань, у тому числі захисту від загроз громадській безпеці чи запобігання цим загрозам;

e) інших важливих цілей загального суспільного інтересу Союзу або держави-члена, зокрема важливого економічного чи фінансового інтересу Союзу або держави-члена, в тому числі питань валютної, бюджетної і податкової політики, охорони громадського здоров'я та соціального забезпечення;

f) захисту незалежності судових органів і судових процесів;

g) запобігання, розслідування, виявлення або переслідування за порушення етичних норм для регульованих професій;

h) моніторингу, перевірки чи регуляторної функції, пов'язаної, навіть періодично, з реалізацією офіційних повноважень у випадках, вказаних у пп. *a–e* та *g*;

i) захисту суб'єкта даних або прав і свобод інших осіб;

j) виконання цивільно-правових позовів.

2. Зокрема, будь-який законодавчий інструмент, вказаний у параграфі 1, повинен містити спеціальні положення, за необхідності, принаймні щодо:

a) цілей опрацювання чи категорій опрацювання;

b) категорій персональних даних;

c) обсягу запроваджених обмежень;

d) гарантій запобігання зловживанню чи незаконному доступу або передаванню;

e) детальної інформації щодо контролера або категорій контролерів;

f) періодів зберігання та застосовних гарантій, з огляду на специфіку, обсяг та цілі опрацювання чи категорії опрацювання;

g) ризиків для прав і свобод суб'єктів даних; або

h) права суб'єктів даних бути повідомленими про обмеження, за винятком порушень цілі обмеження.

Розділ IV. Контролер і оператор

Секція 1

Загальні обов'язки

Стаття 24

Відповідальність контролера

1. Зважаючи на специфіку, обсяг, контекст і цілі опрацювання, а також ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, контролер повинен вжити необхідних технічних і організаційних заходів для того, щоб гарантувати та бути здатним довести, що опрацювання здійснюють згідно з цим Регламентом. За необхідності, такі заходи необхідно переглядати та оновлювати.

2. У разі їх пропорційності щодо опрацювання даних, вказані в параграфі 1 заходи повинні передбачати реалізацію відповідних політик щодо захисту даних контролером.

3. Дотримання затверджених кодексів поведінки, як вказано в ст. 40, чи затверджених механізмів сертифікації, як вказано в ст. 42, можна використовувати як аргумент для підтвердження відповідності обов'язкам контролера.

Стаття 25

Захист даних за призначенням і за замовчуванням

1. Зважаючи на сучасний рівень розвитку, витрати на реалізацію, специфіку, обсяг, контекст і цілі опрацювання, а також ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, які може спричинити опрацювання, контролер повинен, у момент визначення засобів опрацювання та в момент самого опрацювання, вжити необхідних технічних і організаційних заходів, таких як використання псевдонімів, призначених для результативної реалізації принципів захисту даних, зокрема, мінімізації даних, і включення необхідних гарантій до опрацювання для досягнення відповідності вимогам цього Регламенту та забезпечення захисту прав суб'єктів даних.

2. Контролер повинен вжити відповідних технічних і організаційних заходів для гарантування того, що за замовчу-

ванням опрацьовують лише необхідні для кожної спеціальної цілі опрацювання персональні дані. Такий обов'язок застосовують до кількості зібраних персональних даних, ступеня їх опрацювання, періоду їх зберігання та їх доступності. Зокрема, такі заходи повинні гарантувати ненадання за замовчуванням доступу до персональних даних без звернення особи до невизначеної кількості фізичних осіб.

3. Затверджений механізм сертифікації, відповідно до ст. 42, можна використовувати як елемент підтвердження відповідності вимогам, викладеним у п. 1 та 2 цієї статті.

Стаття 26

Спільні контролери

1. Якщо два чи декілька контролерів спільно визначають цілі та засоби опрацювання, вони є спільними контролерами. Вони повинні на умовах прозорості визначити свої обов'язки, що відображають зміст зобов'язань за цим Регламентом, зокрема, щодо реалізації прав суб'єкта даних і надання інформації, вказаних у ст. 13 і 14, шляхом досягнення домовленості між ними, за винятком випадків, стосовно яких відповідні обов'язки контролерів не визначені законодавством Союзу або держави-члена, чинність якого поширюється на контролерів. За домовленістю можна призначити координаційний центр для суб'єктів даних.

2. Домовленість, зазначена в п. 1, повинна належним чином відображати відповідні ролі та відносини спільних контролерів щодо суб'єктів даних. Про суть домовленості необхідно повідомити суб'єктам даних.

3. Незалежно від умов домовленості, окреслених у п. 1, суб'єкт даних може скористатися своїми правами за цим Регламентом щодо контролерів і проти кожного з них.

Стаття 27

Представники контролерів або операторів, які не мають осідків у Союзі

1. У разі застосування ст. 3 (2) контролер або оператор повинен призначити в письмовій формі представника в Союзі.

2. Обов'язок, передбачений у п. 1 цієї статті, не застосовують до:

a) опрацювання, призначеного для окремого випадку, коли воно не передбачає, у великих обсягах, опрацювання спеціальних категорій даних, як вказано в ст. 9 (1), або опрацювання даних про судимості і кримінальні злочини, вказані в ст. 10, та ймовірно не призведе до виникнення ризику для прав і свобод фізичних осіб, з огляду на специфіку, контекст, масштаб і цілі опрацювання; або

b) органу чи установи публічної влади.

3. Представник має осідок в одній з держав-членів, де перебувають суб'єкти даних, чиї персональні дані опрацьовують у зв'язку з пропонуванням їм товарів чи послуг, або чию поведінку відстежують.

4. Представник отримує мандат від контролера або оператора, за яким до нього можуть звертатися, окрім або замість контролера чи оператора, зокрема, наглядові органи і суб'єкти даних, з усіх питань, пов'язаних з опрацюванням, з метою забезпечення відповідності цьому Регламенту.

5. Призначати представника контролером або оператором необхідно без обмеження судових позовів, які могли бути ініційовані проти контролера або оператора як таких.

Стаття 28

Оператор

1. У разі здійснення опрацювання від імені контролера контролер повинен залучити лише тих операторів, які надають достатні гарантії щодо вжиття необхідних технічних і організаційних заходів у спосіб, що дозволяє забезпечити відповідність опрацювання вимогам цього Регламенту та гарантувати захист прав суб'єкта даних.

2. Оператор не повинен залучати будь-якого додаткового оператора, не отримавши попередньо спеціальний чи загальний письмовий дозвіл контролера. Отримавши загальний письмовий дозвіл, оператор повинен повідомити контролера про будь-які цілеспрямовані зміни з метою залучення додаткового чи заміни інших операторів, таким чином надаючи контролеру можливість заперечити проти таких змін.

3. Опрацювання оператором повинен регулювати договір або інший нормативно-правовий акт відповідно до законодавства Союзу або держави-члена, який пов'язує оператора зобов'язальними відносинами з контролером і визначає предмет і тривалість опрацювання, специфіку та цілі опрацювання, тип персональних даних і категорії суб'єктів даних, обов'язки і права контролера. Такий договір або інший нормативно-правовий акт передбачає, зокрема, що оператор:

a) опрацьовує персональні дані лише на підставі задокументованих вказівок контролера, в тому числі щодо передавання персональних даних до третьої країни чи міжнародної організації, за винятком випадку, коли законодавство Союзу або держави-члена містить вимогу, яка поширюється на оператора; у такому випадку оператор інформує контролера про таку законодавчу вимогу перед початком опрацювання, за винятком ситуації, коли законодавством заборонено надання такої інформації на вагомій підставі суспільного інтересу;

b) забезпечує, щоб особи, які отримали дозвіл на опрацювання персональних даних, взяли на себе обов'язок збереження конфіденційності чи були зобов'язані відповідним статутним обов'язком зберігати конфіденційність;

c) вживає усіх заходів, передбачених ст. 32;

d) дотримується вказаних у п. 2 і 4 умов щодо залучення додаткового оператора;

e) враховуючи специфіку опрацювання, допомагає, наскільки це можливо, контролеру належними технічними та організаційними заходами відповідати на запити щодо реалізації прав суб'єкта даних, передбачених у розділі III;

f) допомагає контролеру в забезпеченні відповідності обов'язкам, згідно зі ст. 32–36, з урахуванням специфіки опрацювання та наявної в контролера інформації;

g) на розсуд контролера, вилучає або повертає усі персональні дані контролеру після постачання послуг, пов'язаних з опрацюванням, і вилучає усі копії, за винятком випадків, коли законодавство Союзу або держави-члена містить вимогу збереження персональних даних;

h) надає контролеру всю інформацію, необхідну для підтвердження дотримання зобов'язань, встановлених у цій статті, та сприяння перевіркам, у тому числі інспекціям, які проводять контролер чи інший аудитор відповідно до мандату, наданого контролером.

З урахування пп. *h* п. 1, оператор негайно інформує контролера, якщо, на його думку, вказівка порушує цей Регламент чи інші положення законодавства Союзу або держави-члена щодо захисту даних.

4. У разі залучення оператором додаткового оператора до спеціального опрацювання даних від імені контролера ті самі обов'язки щодо захисту даних, які покладено на контролера або оператора, згідно з договором або іншим нормативно-правовим актом, як зазначено в п. 3, необхідно покласти на такого додаткового оператора договором або іншим нормативно-правовим актом, відповідно до законодавства Союзу або держави-члена, зокрема, шляхом надання достатніх гарантій для вжиття необхідних технічних і організаційних заходів у спосіб, який дозволяє забезпечити відповідність опрацювання вимогам цього Регламенту. Якщо такий додатковий оператор не виконує обов'язки із захисту даних, первинний оператор залишається повністю відповідальним перед контролером за виконання обов'язків додаткового оператора.

5. Дотримання оператором затвердженого кодексу поведінки, як зазначено в ст. 40, чи затвердженого механізму сертифікації, як зазначено в ст. 42, можна використовувати як елемент підтвердження достатніх гарантій, відповідно до п. 1 та 4 цієї статті.

6. Без обмеження окремого договору між контролером і оператором договір або інший нормативно-правовий акт, згадані в п. 3 і 4 цієї статті, можуть ґрунтуватися, загалом чи частково, на стандартних договірних положеннях, викладених у п. 7 і 8 цієї статті, в тому числі, якщо вони є частиною сертифікації, наданої контролеру або оператору відповідно до ст. 42 і 43.

7. Комісія може запроваджувати стандартні договірні положення з питань, викладених у п. 3 і 4 цієї статті, та відповідно до експертної процедури, описаної в ст. 93 (2).

8. Наглядовий орган може ухвалити стандартні договірні положення з питань, викладених у п. 3 і 4 цієї статті, та відповідно до механізму послідовності, зазначеного в ст. 63.

9. Договір або інший нормативно-правовий акт, як зазначено в п. 3 і 4, повинні бути оформлені в письмовій формі, в тому числі в електронній.

10. З дотриманням положень ст. 82, 83 і 84 у разі порушення оператором цього Регламенту шляхом визначення цілей і засобів опрацювання оператора необхідно вважати контролером для цілей такого опрацювання.

Стаття 29

Опрацювання під керівництвом контролера або оператора

Оператор або будь-яка особа, яка діє під керівництвом контролера чи оператора і має доступ до персональних даних, не повинна опрацьовувати такі дані без інструкцій контролера, за винятком випадків, передбачених законодавством Союзу або держави-члена.

Стаття 30

Записи опрацювання даних

1. Кожний контролер і, за необхідності, представник контролера повинні вести запис про опрацювання даних, що належать до його сфери відповідальності. Такий запис повинен містити всю інформацію про:

a) особу та контактні дані контролера та, за необхідності, об'єднаного контролера, представника контролера та співробітника з питань захисту даних;

b) цілі цього Регламенту;

c) категорії суб'єктів даних і категорії персональних даних;

d) категорії одержувачів, яким персональні дані були або будуть розкриті, в тому числі одержувачів у третіх країнах або міжнародні організації;

e) за необхідності, передавання персональних даних третій країні або міжнародній організації, в тому числі ідентифікацію такої третьої країни чи міжнародної організації та, в разі

актів передавання, згаданих у пп. 2 ст. 49 (1), документацію відповідних гарантій;

f) за можливості, – передбачені часові обмеження для вилучення різних категорій даних;

g) за можливості, – загальний опис технічних і організаційних заходів безпеки, зазначених у ст. 32 (1).

2. Кожний оператор і, за необхідності, представник оператора повинні вести запис про усі категорії опрацювання, здійснювані від імені контролера, що включає інформацію про:

a) особу та контактні дані оператора чи операторів і кожного контролера, від імені якого діє оператор, та, за необхідності, представника контролера або представника оператора та співробітника з питань захисту даних;

b) категорії опрацювання, яке здійснюють від імені кожного контролера;

c) за необхідності, передавання персональних даних третій країні або міжнародній організації, в тому числі ідентифікацію такої третьої країни чи міжнародної організації та, в разі актів передавання, згаданих у другому підпункті ст. 49 (1), документацію відповідних гарантій;

d) за можливості, – загальний опис технічних і організаційних заходів безпеки, зазначених у ст. 32 (1).

3. Записи, згадані в п. 1 і 2, повинні бути оформлені в письмовій формі, в тому числі електронній.

4. Контролер або оператор і, за необхідності, представник контролера або оператора повинні надавати запис на запит наглядового органу.

5. Обов'язки, окреслені в п. 1 і 2, не покладаються на підприємства чи організації з кількістю працівників, меншою за 250 осіб, за винятком випадків, коли здійснюване опрацювання може призвести до виникнення ризику для прав і свобод суб'єктів даних, призначене для окремого випадку, або якщо опрацювання передбачає спеціальні категорії даних, як зазначено в ст. 9 (1), або персональні дані про судимості і кримінальні злочини, згадані в ст. 10.

Стаття 31

Співпраця із наглядовим органом

Контролер і оператор та, за необхідності, їхні представники, виконуючи свої завдання, повинні співпрацювати з наглядовим органом.

Секція 2

Безпека персональних даних

Стаття 32

Безпека опрацювання

1. Враховуючи сучасний рівень розвитку, витрати на реалізацію, специфіку, обсяги, контекст і цілі опрацювання, а також ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, які викликає опрацювання, контролер і оператор повинні вжити необхідних технічних і організаційних заходів для забезпечення рівня безпеки відповідно до ризику, в тому числі у належних випадках:

a) використання псевдонімів і шифрування персональних даних;

b) здатність забезпечувати безперервну конфіденційність, цілісність, наявність і стійкість систем і послуг опрацювання;

c) здатність вчасно відновити персональні дані у разі технічної аварії і надати доступ до них;

d) регулярність тестування, оцінювання та аналізу результативності технічних і організаційних заходів для гарантування безпеки опрацювання.

2. Оцінюючи рівень безпеки, необхідно враховувати, зокрема, ризики, пов'язані з опрацюванням, зокрема такі, що виникають внаслідок випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, які передано, збережено або іншим чином опрацьовано.

3. Дотримання затверджених кодексів поведінки, як зазначено в ст. 40, чи затверджених механізмів сертифікації, як вказано в ст. 42, може слугувати підтвердженням відповідності вимогам, викладеним у п. 1 цієї статті.

4. Контролер і оператор повинні вжити заходів для того, щоб будь-яка фізична особа, яка діє під керівництвом контролера або оператора і має доступ до персональних даних, не могла опрацьовувати їх, за винятком випадків, коли вона здійснює це за інструкціями контролера або коли вона зобов'язана діяти таким чином відповідно до законодавства Союзу або держави-члена.

Стаття 33

Нотифікація наглядового органу про порушення захисту персональних даних

1. У разі порушення захисту персональних даних контролер повинен без необґрунтованої затримки та, за можливості, не пізніше ніж протягом 72 годин після того, як йому стало відомо про це, повідомити про порушення захисту персональних даних компетентний наглядовий орган, якщо таке порушення загрожує ризиком для прав і свобод фізичних осіб. Якщо наглядовий орган не повідомлено протягом 72 годин, необхідно надати супровідну інформацію про причини затримки.

2. Оператор повинен повідомити контролера без необґрунтованої затримки після того, як йому стало відомо про порушення захисту персональних даних.

3. У повідомленні, згаданому в п. 1, треба подати таку інформацію:

a) описати специфіку порушення захисту персональних даних, у тому числі, за можливості, категорії та приблизну кількість зацікавлених суб'єктів даних і категорії та приблизну кількість записів персональних даних, яких це стосується;

b) назвати особу та повідомити контактні дані співробітника з питань захисту даних або іншого координаційного органу, де можна отримати більше інформації;

c) описати ймовірні наслідки порушення захисту персональних даних;

d) описати заходи, яких ужив чи запропонував ужити контролер у відповідь на порушення захисту персональних даних, у тому числі, в разі необхідності, заходи для зниження його потенційних негативних наслідків.

4. Якщо і оскільки надати інформацію одночасно неможливо, її можна надавати поетапно, без подальших необґрунтованих затримок.

5. Контролер повинен фіксувати будь-які порушення захисту персональних даних, факти порушення захисту персональних даних, їх наслідки і вжиті для виправлення ситуації заходи. Задокументована така інформація дає можливість наглядовому органу перевірити відповідність цій статті.

Стаття 34

Повідомлення суб'єкта даних про порушення захисту персональних даних

1. Якщо порушення захисту персональних даних загрожує високими ризиками для прав і свобод фізичних осіб, контролер повинен повідомити суб'єкта даних про порушення захисту персональних даних без необґрунтованої затримки.

2. Повідомлення суб'єкта даних, згадане в п. 1 цієї статті, повинно містити опис з використанням чітких і простих формулювань, специфіки порушення захисту персональних даних та інформацію про заходи, вказані в пп. *b*, *c* і *d* ст. 33 (3).

3. Повідомляти суб'єкта даних не обов'язково у разі виконання однієї з таких вимог:

a) контролер вжив необхідних технічних та організаційних заходів захисту, і такі заходи застосовано до персональних даних, на які вплинуло порушення захисту персональних даних, зокрема ті, що унеможливлюють розуміння персональних даних будь-якою особою, яка не має дозволу на доступ до них, наприклад, шифрування;

b) контролер вжив заходів, які гарантують, що високий ризик для прав і свобод суб'єктів даних, згаданий у п. 1, ймовірно, більше не виникне;

c) повідомлення передбачає докладання надмірних зусиль. У такому разі замість нього використовують публічне повідомлення чи подібний інструмент, за допомогою якого інформують суб'єктів даних рівноцінно дієвим способом.

4. Якщо контролер ще не повідомив суб'єктові даних про порушення захисту персональних даних, наглядовий орган,

зваживши ймовірність спричинення порушенням захисту персональних даних високого ризику, може вимагати зробити це чи може вирішити, що будь-яку з умов, перелічених у п. 3, виконано.

Секція 3

Оцінювання впливу на захист даних і попередня консультація

Стаття 35

Оцінювання впливу на захист даних

1. Якщо тип опрацювання, зокрема, з використанням нових технологій і зважаючи на специфіку, обсяг, контекст і цілі опрацювання, ймовірно призведе до виникнення високого ризику для прав і свобод фізичних осіб, контролер, перед опрацюванням, повинен оцінити вплив передбачених операцій з опрацювання на захист персональних даних. Одне оцінювання може стосуватися низки подібних операцій опрацювання, що можуть спричиняти подібні високі ризики.

2. Контролер повинен звернутися за рекомендаціями до фахівця з питань захисту даних, якщо його призначено у ході проведення оцінювання впливу на захист даних.

3. Оцінювання впливу на захист даних, згідно п. 1, необхідне, зокрема, у таких випадках:

a) систематичного та масштабного оцінювання персональних аспектів, що стосуються фізичних осіб, яке ґрунтується на автоматизованому опрацюванні, в тому числі профайлінгу, та на яке спирається рішення, що мають юридичні наслідки щодо фізичної особи чи подібним чином істотно впливають на фізичну особу;

b) широкомасштабного опрацювання спеціальних категорій даних, згаданих у ст. 9 (1), та персональних даних про судимості і кримінальні злочини, вказані в ст. 10; або

c) систематичного та широкомасштабного моніторингу зони, що перебуває у відкритому доступі.

4. Наглядовий орган повинен розробити та оприлюднити перелік операцій опрацювання, на які поширюється вимога

проведення оцінювання впливу на захист даних, відповідно до п. 1. Наглядовий орган повідомляє Раду про такі переліки, як зазначено в ст. 68.

5. Наглядовий орган може також розробляти й оприлюднювати перелік операцій опрацювання, на які не поширюється вимога проведення оцінювання впливу на захист даних. Наглядовий орган повинен повідомляти Раду про такі переліки.

6. Ухвалюючи переліки, згідно з п. 4 і 5, компетентний наглядовий орган повинен застосовувати механізм послідовності, вказаний у ст. 63, якщо такі переліки включають опрацювання даних, пов'язане з пропонуванням товарів або послуг суб'єктам даних або моніторингом їхньої поведінки в декількох державах-членах, або можуть істотно впливати на вільне переміщення персональних даних у межах Союзу.

7. Оцінювання повинне містити принаймні такі елементи:

a) систематичний опис передбачених операцій опрацювання та цілей опрацювання, в тому числі, за необхідності, законного інтересу контролера;

b) оцінювання необхідності та пропорційності операцій опрацювання щодо цілей;

c) оцінювання ризиків для прав і свобод суб'єктів даних, вказаних у п. 1; та

d) заходи, передбачені для боротьби з ризиками, в тому числі, гарантії, заходи безпеки та механізми забезпечення захисту персональних даних і доведення відповідності цьому Регламенту, з урахуванням прав і законних інтересів суб'єктів даних та інших залучених осіб.

8. Необхідно належним чином враховувати дотримання відповідними контролерами або операторами затверджених кодексів поведінки, вказаних у ст. 40 під час оцінювання впливу операцій опрацювання, які здійснюють такі контролери або оператори, зокрема, для цілей оцінювання впливу на захист даних.

9. У разі необхідності контролер повинен ознайомитися з думками суб'єктів даних або їхніх представників про заплановане опрацювання, без обмеження захисту комерційних або суспільних інтересів або безпеки операцій опрацювання.

10. Якщо законодавчою базою опрацювання, відповідно до пп. *c* або *e* ст. 6 (1), є законодавство Союзу або законодавство держави-члена, яке поширюється на контролера, таке законодавство регулює конкретну операцію опрацювання чи відповідну низку операцій, і якщо оцінювання впливу на захист даних вже було здійснене як частина загального оцінювання впливу в контексті ухвалення такої законодавчої бази, п. 1–7 не застосовують, за винятком випадків, коли держави-члени вважають за необхідне провести таке оцінювання перед опрацюванням даних.

11. У разі необхідності контролер повинен провести перевірку, щоб пересвідчитися, чи відбувається опрацювання з урахуванням результатів оцінювання впливу на захист даних, принаймні, у разі зміни ризику, який становлять операції опрацювання.

Стаття 36

Попередня консультація

1. Контролер повинен надати консультацію наглядовому органу перед початком опрацювання, якщо оцінка впливу на захист даних, згідно зі ст. 35, свідчить про те, що опрацювання спричинить високий ризик, якщо контролер не вживатиме заходів для його зниження.

2. Якщо наглядовий орган вважає, що заплановане опрацювання, вказане в п. 1, може порушити цей Регламент, зокрема, якщо контролер недостатньо ідентифікував або знизив ризик, наглядовий орган протягом восьми тижнів після отримання запиту на консультацію повинен надати контролеру письмові рекомендації та, в разі необхідності, оператору, а також може використовувати будь-які свої повноваження, вказані в ст. 58. Цей період може бути подовжено на шість тижнів з огляду на складність запланованого опрацювання. Наглядовий орган інформує контролера та, в разі необхідності, оператора про будь-яке таке подовження протягом одного місяця з дати отримання запиту на консультацію разом з інформацією про причини затримки. Термін може бути призупинено до отримання наглядовим органом інформації, яку він запросив для цілей консультації.

3. Надаючи консультацію наглядовому органу, відповідно до п. 1, контролер повинен надати таку інформацію:

a) в разі необхідності, інформацію про відповідні обов'язки контролера, об'єднаних контролерів і операторів, залучених до опрацювання, зокрема, до опрацювання в межах групи підприємств;

b) про цілі та засоби запланованого опрацювання;

c) про засоби та гарантії, передбачені для захисту прав і свобод суб'єктів даних, відповідно до цього Регламенту;

d) в разі необхідності, контактні дані з питань захисту даних;

e) про оцінку впливу на захист даних, передбачену в ст. 35; і

f) будь-яку іншу інформацію, яку запитує наглядовий орган.

4. Держави-члени повинні надати наглядовому органу консультацію під час підготування пропозиції до законодавчого акта національного рівня, або до регуляторного інструменту на підставі такого законодавчого акта, що стосується опрацювання.

5. Без обмеження положень п. 1 законодавство держав-членів може вимагати від контролерів надавати консультації та отримувати від наглядового органу попередній дозвіл на опрацювання контролером з метою реалізації завдання, яке контролер виконує для задоволення суспільного інтересу, в тому числі опрацювання в сфері соціального захисту і охорони суспільного здоров'я.

Секція 4

Співробітник з питань захисту даних

Стаття 37

Призначення співробітника з питань захисту даних

1. Контролер і оператор призначають співробітника з питань захисту даних у будь-якому з перелічених випадків:

a) опрацювання здійснює публічний орган або установа, за винятком судів, що діють як судові інстанції;

b) основними видами діяльності контролера або оператора є операції опрацювання, які, з урахуванням їх специфіки, обсягів та/чи цілей, вимагають регулярного, систематичного і широкомасштабного моніторингу суб'єктів даних; або

c) основними видами діяльності контролера або оператора є широкомасштабне опрацювання спеціальних категорій даних, відповідно до ст. 9, і персональних даних про судимості і кримінальні злочини, вказані в ст. 10.

2. Група підприємств може призначити одного співробітника з питань захисту даних за умови, що кожен осідок має доступ до цього.

3. Якщо контролер або оператор є публічним органом або установою, одного співробітника з питань захисту даних можна призначати для декількох таких органів або установ, з урахуванням їх організаційної структури та розмірів.

4. У ситуаціях, відмінних від згаданих у п. 1, контролер або оператор чи асоціації та інші органи, що представляють категорії контролерів або операторів, можуть або, відповідно до вимог законодавства Союзу чи держави-члена, повинні призначити співробітника з питань захисту даних. Співробітник з питань захисту даних може працювати на такі асоціації та інші органи, що представляють контролерів або операторів.

5. Співробітника з питань захисту даних призначають з урахуванням професійних якостей і, зокрема, експертних знань із права та практики захисту даних, а також здатності виконувати завдання, перелічені в ст. 39.

6. Співробітник з питань захисту даних може бути штатним працівником контролера або оператора або виконувати завдання на підставі договору про надання послуг.

7. Контролер або оператор повинен опублікувати контактні дані співробітника з питань захисту даних і повідомити їх наглядовому органу.

Стаття 38

Позиція співробітника з питань захисту даних

1. Контролер і оператор забезпечують, щоб співробітника з питань захисту даних залучали, належним чином і вчасно, до усіх питань, що стосуються захисту персональних даних.

2. Контролер і оператор надають підтримку співробітнику з питань захисту даних у виконанні завдань, перелічених у ст. 39, шляхом надання ресурсів, необхідних для реалізації таких завдань, і доступу до персональних даних, операцій опрацювання та підтримання рівня його експертних знань.

3. Контролер і оператор забезпечують, щоб співробітник з питань захисту даних не отримував жодних інструкцій щодо виконання цих завдань. Контролер або оператор не має права відсторонити або оштрафувати таку особу за неналежне виконання її завдань. Співробітник з питань захисту даних безпосередньо підзвітний найвищому управлінському органу контролера або оператора.

4. Суб'єкти даних можуть звертатися до співробітника з питань захисту даних щодо усіх питань, пов'язаних з опрацюванням їхніх персональних даних і реалізацією їхніх прав за цим Регламентом.

5. Співробітник з питань захисту даних зобов'язаний зберігати таємницю або конфіденційність щодо виконання своїх завдань, відповідно до законодавства Союзу або держави-члена.

6. Співробітник з питань захисту даних може виконувати інші завдання та обов'язки. Контролер або оператор забезпечують, щоб жодні такі завдання та обов'язки не спричинили конфлікту інтересів.

Стаття 39

Завдання співробітника з питань захисту даних

1. Співробітник з питань захисту даних має щонайменше такі завдання:

a) інформувати та надавати рекомендації контролеру або оператору і працівникам, які здійснюють опрацювання, щодо їхніх обов'язків відповідно до цього Регламенту та інших положень про захист даних Союзу чи держави-члена;

b) здійснювати моніторинг відповідності цього Регламенту іншим положенням про захист даних Союзу або держави-члена та політиці контролера або оператора щодо захисту персональних даних, у тому числі щодо розподілу обов'язків, підвищення обізнаності та підготовки персоналу, залученого до операцій опрацювання, та відповідних перевірок;

c) на запит надавати рекомендації щодо оцінювання впливу на захист даних і здійснювати його моніторинг, відповідно до ст. 35;

d) співпрацювати із наглядовим органом;

e) діяти як координаційний центр наглядового органу з питань, що стосуються опрацювання, в тому числі попередніх консультацій, вказаних у ст. 36, і надавати консультації, за необхідності, щодо будь-якого іншого питання.

2. Під час виконання своїх обов'язків співробітник з питань захисту даних повинен належним чином враховувати ризик, пов'язаний з операціями опрацювання, специфіку, обсяг, контекст і цілі опрацювання.

Секція 5

Кодекси поведінки та сертифікація

Стаття 40

Кодекс поведінки

1. Держави-члени, наглядові органи, Рада і Комісія заохочують розроблення кодексів поведінки, спрямованих на сприяння належному застосуванню цього Регламенту, з урахуванням особливостей характеристики різних секторів опрацювання та конкретних потреб мікропідприємств, малих і середніх підприємств.

2. Асоціації та інші органи, що представляють категорії контролерів або операторів можуть підготувати кодекси поведінки або внести зміни і доповнення чи розширити чинні кодекси з метою уточнення застосування цього Регламенту, зокрема, щодо:

a) правомірного та прозорого опрацювання;

b) законних інтересів контролерів у конкретних ситуаціях;

c) збирання персональних даних;

d) використання псевдонімів для персональних даних;

e) інформації, яку надають громадськості та суб'єктам даних;

f) реалізації прав суб'єктів даних;

g) інформації, яку надають дітям, щодо їхнього захисту і способу, яким необхідно отримувати згоду носіїв батьківської відповідальності щодо дітей;

h) заходів і процедур, вказаних у ст. 24 і 25, і заходів з гарантування безпеки опрацювання, вказаних у ст. 32;

i) повідомлення наглядових органів про порушення захисту персональних даних і повідомлення суб'єктів даних про такі порушення захисту персональних даних;

j) передавання персональних даних до третіх країн або міжнародних організацій; або

k) позасудових процедур чи інших процедур щодо врегулювання суперечок для врегулювання спорів між контролерами та суб'єктами даних у зв'язку з опрацюванням, без порушення прав суб'єктів даних, відповідно до ст. 77 і 79.

3. Кодекси поведінки, що затверджені, відповідно до п. 5 цієї статті, та мають загальну дію, відповідно до п. 9 цієї статті, також можна застосовувати до контролерів або операторів, на яких не поширюється чинність цього Регламенту, відповідно до ст. 3 для того, щоб надати належні гарантії в межах передавання персональних даних до третіх країн чи міжнародних організацій на умовах, наведених у пп. *e* ст. 46 (2). Такі контролери або оператори повинні взяти на себе зобов'язання, які є обов'язковими і можливими для виконання, за допомогою договірних або інших юридично зобов'язальних інструментів, застосувати зазначені належні гарантії, у тому числі гарантії щодо прав суб'єктів даних.

4. Кодекс поведінки, вказаний у п. 2 цієї статті, повинен передбачати механізми, що дозволяють органу, вказаному в ст. 41 (1), здійснювати обов'язковий моніторинг дотримання його положень контролерами або операторами, які взяли на себе зобов'язання щодо його застосування, без обмеження завдань і повноважень наглядових органів, що є компетентними, відповідно до ст. 55 або 56.

5. Асоціації та інші органи, вказані в п. 2 цієї статті, що мають намір підготувати кодекс поведінки чи внести зміни та доповнення до чинного кодексу, подають проект кодексу,

змін і доповнень або розширення до наглядового органу, що є компетентним, відповідно до ст. 55. Наглядовий орган надає висновок про те, чи відповідає проект кодексу, змін і доповнень або розширення цьому Регламенту, та затверджує такий проект кодексу, змін і доповнень або розширення, якщо з'ясує, що в ньому передбачено достатні належні гарантії.

6. Якщо проект кодексу, змін і доповнень або розширення затверджено, відповідно до п. 5, та якщо відповідний кодекс поведінки не стосується опрацювання даних у декількох державах-членах, наглядовий орган реєструє й публікує кодекс.

7. Якщо проект кодексу стосується опрацювання даних у декількох державах-членах, наглядовий орган, що є компетентним, відповідно до ст. 55, перш ніж затвердити проект кодексу, змін, доповнень або розширення, подає його на процедуру, вказану в ст. 63, до Ради, яка надає висновок щодо того, чи відповідає проект кодексу, змін та доповнень або розширення цьому Регламенту або, в ситуації, передбаченій п. 3 цієї статті, чи закладено в ньому належні гарантії.

8. Якщо висновок, вказаний у п. 7, підтверджує, що проект кодексу, змін і доповнення або розширення відповідає цьому Регламенту або, в ситуації, вказаній у п. 3 цієї статті, передбачає належні гарантії, Рада подає свій висновок до Комісії.

9. Комісія може, за допомогою імплементаційних актів, вирішити, що затверджений кодекс поведінки, змін і доповнень або розширення, подані їй відповідно до п. 8 цієї статті, мають загальну дію в межах Союзу. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, встановленої в ст. 93 (2).

10. Комісія забезпечує належну публічність затвердженим кодексам, щодо яких було ухвалено рішення про те, що вони мають загальну дію, згідно з п. 9.

11. Рада впорядковує усі затверджені кодекси поведінки, зміни та доповнення або розширення у формі реєстру й оприлюднює їх за допомогою належних засобів.

Стаття 41

Моніторинг затверджених кодексів поведінки

1. Без обмеження завдань і повноважень компетентного наглядового органу за ст. 57 і 58 моніторинг дотримання кодексу поведінки, відповідно до ст. 40, може здійснювати орган, який володіє належним рівнем експертних знань у сфері предмета кодексу та акредитований для такої цілі компетентним наглядовим органом.

2. Орган, як зазначено в п. 1, може бути акредитований для моніторингу дотримання кодексу поведінки, якщо він:

a) довів свою незалежність та експертні знання в сфері предмета кодексу за повного виконання вимог компетентного наглядового органу;

b) запровадив процедури, що дозволяють йому провадити оцінювання правоздатності залучених контролерів і операторів для застосування кодексу, моніторингу дотримання ними його положень та періодичного перегляду його дії;

c) запровадив процедури та структури для розгляду скарг щодо порушень кодексу чи способу, у який застосовано кодекс або який застосовує контролер або оператор, та надання таким процедурам і структурам прозорості для суб'єктів даних і громадськості; та

d) довів, за повного виконання вимог компетентного наглядового органу, що його завдання та обов'язки не спричиняють конфлікту інтересів.

3. Компетентний наглядовий орган подає проект критеріїв для акредитації органу, як вказано в п. 1 цієї статті, до Ради, відповідно до механізму послідовності, вказаного в ст. 63.

4. Без порушення завдань і повноважень компетентного наглядового органу та положень розділу VIII, орган, як вказано в п. 1 цієї статті, з урахуванням належних гарантій, вживає необхідних заходів у разі порушення кодексу контролером або оператором, у тому числі призупиняє роботу чи відстороняє залученого контролера або оператора. Про такі свої дії та їх підстави він повідомляє компетентний наглядовий орган.

5. Компетентний наглядовий орган відкликає акредитацію органу, як вказано в п. 1, якщо умови для акредитації не

виконано чи більше не виконуються, або якщо дії, яких вживає орган, суперечать цьому Регламенту.

6. Цю статтю не застосовують до опрацювання, яке здійснюють публічні органи.

Стаття 42

Сертифікація

1. Держави-члени, наглядові органи, Рада і Комісія заохочують, зокрема на рівні Союзу, запровадження механізмів сертифікації захисту даних, штампів і знаків захисту даних з метою підтвердження відповідності цьому Регламенту операцій опрацювання, які здійснюють контролери і оператори. Необхідно враховувати особливі потреби мікропідприємств, малих і середніх підприємств.

2. Механізми сертифікації захисту даних, штампи і знаки, затверджені відповідно до п. 5 цієї статті, можна запровадити з метою підтвердження наявності належних гарантій, які надають контролери або оператори, на яких не поширюється чинність цього Регламенту, відповідно до ст. 3, у межах передавання персональних даних до третіх країн чи міжнародних організацій на умовах, вказаних у пп. *f* ст. 46 (2). Такі контролери або оператори повинні взяти на себе зобов'язання, які є обов'язковими і можливими для виконання, за допомогою договірних або інших юридично зобов'язальних інструментів, для того, щоб застосувати зазначені належні гарантії, у тому числі гарантії щодо прав суб'єктів даних.

3. Сертифікація є добровільною і доступною шляхом реалізації прозорого процесу.

4. Сертифікація, відповідно до цієї статті, не знижує ступеня відповідальності контролера або оператора за дотримання цього Регламенту та не обмежує завдання і повноваження наглядових органів, що є компетентними, відповідно до ст. 55 чи 56.

5. Сертифікацію, відповідно до цієї статті, видають органи сертифікації, вказані в ст. 43, або компетентні наглядові органи на підставі критеріїв, затверджених таким компетентним наглядовим органом, згідно зі ст. 58 (3), або Радою, згідно зі ст. 63.

Якщо критерії затверджено Радою, це може стати результатом запровадження спільної сертифікації, Європейського штампу захисту даних.

6. Контролер або оператор, який подає своє опрацювання до механізму сертифікації, надає органу сертифікації, вказаному в ст. 43, або, у разі необхідності, компетентному наглядовому органу, всю інформацію та доступ до опрацювання даних, необхідні для проведення процедури сертифікації.

7. Сертифікат видають контролеру або оператору на строк до трьох років, він може бути поновлений на тих самих умовах, якщо і надалі буде виконано відповідні вимоги. Сертифікат відкликають, у разі необхідності, органи сертифікації, зазначені в ст. 43, або компетентний наглядовий орган, якщо вимоги для сертифікації не виконано або більше не виконуються.

8. Рада впорядковує усі механізми сертифікації та штампи і знаки захисту даних у формі реєстру й оприлюднює їх за допомогою належних засобів.

Стаття 43

Органи сертифікації

1. Без обмеження завдань і повноважень компетентного наглядового органу за ст. 57 і 58 органи сертифікації, що володіють необхідним рівнем експертних знань у сфері захисту даних, після повідомлення наглядового органу для надання йому можливості здійснювати свої повноваження згідно з пп. *h* ст. 58 (2), у разі необхідності, видають та оновлюють сертифікацію. Держави-члени забезпечують, щоб органи сертифікації були акредитовані одним або обома органами:

a) наглядовим органом, компетенція якого окреслена в ст. 55 чи 56;

b) національним органом з акредитації, названим відповідно до Регламенту Європейського Парламенту і Ради (ЄС) № 765/2008* згідно з EN-ISO/IEC 17065/2012 та додатковими

* Регламент Європейського Парламенту і Ради (ЄС) № 765/2008 від 9 липня 2008 р. про вимоги до акредитації та ринкового нагляду

вимогами, встановленими наглядовим органом, компетенція якого окреслена ст. 55 чи 56.

2. Органи сертифікації, вказані в п. 1, необхідно акредитувати згідно з цим пунктом, лише за умови, що вони:

a) довели свою незалежність та експертні знання в сфері предмета сертифікації за повного виконання вимог компетентного наглядового органу;

b) зобов'язались поважати критерії, вказані в ст. 42 (5) і затверджені наглядовим органом, компетенцію якого визнано згідно зі ст. 55 чи 56 або Радою, відповідно до ст. 63;

c) розробили процедури надання, періодичної перевірки та відкликання сертифіката захисту даних, штампів і знаків;

d) запровадили процедури та структури для розгляду скарг щодо порушень сертифікації чи способу, в який сертифікацію було здійснено чи здійснює контролер або оператор, та для забезпечення прозорості таких процедур і структур для суб'єктів даних і громадськості; та

e) довели, за повного виконання вимог компетентного наглядового органу, що їхні завдання та обов'язки не спричиняють конфлікту інтересів.

3. Акредитацію органів сертифікації, як вказано в п. 1 і 2 цієї статті, здійснюють на підставі критеріїв, затверджених наглядовим органом, компетенцію якого визначено згідно зі ст. 55 чи 56 або Радою, відповідно до ст. 63. У випадку акредитації відповідно до пп. *b* п. 1 цієї статті ці вимоги доповнюють тими, що передбачені в Регламенті (ЄС) № 765/2008, і технічними нормами, що описують методи та процедури органів сертифікації.

4. Органи сертифікації, вказані в п. 1, несуть відповідальність за належне оцінювання, в результаті якого можна видати або відкликати сертифікат без обмеження відповідальності контролера або оператора за дотримання цього Регламенту. Акредитацію видають на строк до п'яти років, її можна понов-

---

стосовно реалізації продуктів та про скасування Регламенту (ЄЕС) № 339/93 (OB L 218, 13.08.2008, с. 30).

лювати на тих самих умовах, якщо орган сертифікації відповідає вимогам, передбаченим цією статтею.

5. Органи сертифікації, вказані в п. 1, повинні надати компетентним наглядовим органам інформацію про причини надання чи відкликання сертифіката, яку запитують.

6. Наглядовий орган повинен у доступній формі оприлюднити вимоги, вказані в п. 3 цієї статті, та критерії, перелічені в ст. 42 (5). Наглядові органи також передають ці вимоги та критерії Раді. Рада впорядковує усі механізми сертифікації та штампи захисту даних у формі реєстру й оприлюднює їх належними засобами.

7. Дотримуючись положень глави VIII, компетентний наглядовий орган або національний орган з акредитації анулює акредитацію органу сертифікації, відповідно до п. 1 цієї статті, якщо вимоги до акредитації виконано чи їх більше не виконують, або якщо заходи, яких вживає орган сертифікації, суперечать положенням цього Регламенту.

8. Комісія повинна мати повноваження ухвалювати делеговані акти, згідно зі ст. 92, з метою уточнення вимог, які необхідно врахувати щодо механізмів сертифікації захисту даних, вказаних у ст. 42 (1).

9. Комісія може ухвалювати імплементаційні акти про технічні стандарти для механізмів сертифікації та штампів і знаків захисту даних, механізмів сприяння та визнання таких механізмів сертифікації, штампів і знаків. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, описаної в ст. 93 (2).

Розділ V. Передавання персональних даних до третіх країн або міжнародних організацій

Стаття 44

Загальні принципи передавання

Будь-яке передавання персональних даних, що перебувають у процесі опрацювання чи призначені для опрацювання після передавання до третьої країни чи міжнародної організації, повинно відбуватися лише у разі, якщо з урахуванням

інших положень цього Регламенту контролер і оператор дотримуються умов, передбачених цим розділом, в тому числі, для наступних актів передавання персональних даних з третьої країни чи міжнародної організації до іншої третьої країни чи міжнародної організації. Усі положення в цій главі застосовують з метою забезпечення захисту фізичних осіб, який гарантує цей Регламент.

Стаття 45

Передавання на підставі рішення про відповідність

1. Передавання персональних даних до третьої країни чи міжнародної організації може відбуватися, якщо Комісія вирішила, що третя країна територія чи один або декілька визначених секторів у межах такої третьої країни або відповідна міжнародна організація забезпечують належний рівень захисту. Таке передавання не вимагає отримання будь-якого спеціального дозволу.

2. Оцінюючи відповідність захисту, Комісія, зокрема, враховує такі елементи:

a) верховенство права, повагу до прав людини та фундаментальних свобод, відповідне законодавство, як загальне, так і секторальне, в тому числі щодо громадської безпеки, оборони, національної безпеки та кримінального права і доступу органів публічної влади до персональних даних, а також імплементацію такого законодавства, норми про захист даних, правила професійної діяльності та заходи з безпеки, в тому числі правила щодо наступного передавання персональних даних до іншої третьої країни чи міжнародної організації, яких дотримуються в такій країні чи міжнародній організації, судову практику, а також дієві права суб'єкта даних, які можна реалізувати, та дієвий адміністративний і судовий захист для суб'єктів даних, чиї персональні дані передають;

b) існування та дієве функціонування незалежних наглядових органів у третій країні чи тих, яким підпорядковується міжнародна організація, із відповідальністю за забезпечення та дотримання норм про захист даних, у тому числі належними правозастосовними повноваженнями, для надання допомоги

та рекомендацій суб'єктам даних під час реалізації їхніх прав і для співпраці з наглядовими органами держав-членів; і

c) міжнародні зобов'язання, які взяли на себе третя країна або відповідна міжнародна організація, або інші зобов'язання, що випливають із юридично зобов'язальних конвенцій або інструментів, а також із їхньої участі в багатосторонніх або регіональних системах, зокрема в сфері захисту персональних даних.

3. Комісія, оцінивши адекватність рівня захисту, може вирішити, у формі імплементаційного акта, що третя країна, територія чи один або декілька визначених секторів у межах третьої країни або міжнародна організація забезпечує належний рівень захисту даних у значенні п. 2 цієї статті. Імплементаційний акт передбачає механізм періодичного перегляду, щонайменше кожні чотири роки, з урахуванням усіх х тенденцій розвитку в третій країні чи міжнародній організації. Імплементаційний акт уточнює територіальне та секторальне застосування та, за необхідності, визначає наглядовий орган або органи, вказані в пп. *b* п. 2 цієї статті. Імплементаційний акт ухвалюють відповідно до експертної процедури, вказаної в ст. 93 (2).

4. Комісія, що працює на постійній основі, здійснює моніторинг тенденцій розвитку в третіх країнах і міжнародних організаціях, які можуть вплинути на рішення, ухвалені відповідно до п. 3 статті, та рішення, ухвалені на підставі ст. 25 (6) Директиви 95/46/ЄС.

5. Якщо наявна інформація свідчить, зокрема після перегляду, як вказано в п. 3 цієї статті, про те, що третя країна, територія чи один або декілька визначених секторів у межах третьої країни, чи міжнародна організація більше не забезпечує належного рівня захисту в значенні п. 2 цієї статті необхідною мірою, комісія скасовує, вносить зміни та доповнення або призупиняє рішення, вказане в п. 3 цієї статті, шляхом ухвалення імплементаційних актів, що не мають зворотної сили. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, описаної в ст. 93 (2).

Зважаючи на належним чином підтверджену термінову необхідність, Комісія повинна негайно ухвалити застосовні імплементаційні акти у порядку, визначеному в ст. 93 (3).

6. Комісія проводить консультації з третьою країною чи міжнародною організацією з метою виправлення ситуації, що призвела до рішення, ухваленого відповідно до п. 5.

7. Рішення, ухвалене відповідно до п. 5 цієї статті, не обмежує передавання персональних даних до третьої країни, території чи одного або декількох визначених секторів у межах такої третьої країни, чи відповідної міжнародної організації, згідно зі ст. 46–49.

8. Комісія публікує в Офіційному віснику Європейського Союзу та розміщує на своїй сторінці в мережі Інтернет список третіх країн, територій і визначених секторів у межах третьої країни та міжнародних організацій, щодо яких було ухвалено рішення про те, що вони більше не забезпечують належного рівня захисту.

9. Рішення, ухвалені Комісією на підставі ст. 25 (6) Директиви 95/46/ЄС, залишаються чинними до внесення до них змін і доповнень, заміни або скасування Рішенням Комісії, ухваленим згідно з п. 3 або 5 цієї статті.

Стаття 46

Передавання з урахуванням належних гарантій

1. За відсутності рішення відповідно до ст. 45 (3) контролер або оператор можуть передавати персональні дані до третьої країни чи міжнародної організації, лише якщо контролер або оператор надав належні гарантії, та за наявності прав суб'єктів даних, що вимагають реалізації, та дієвих засобів правового захисту для суб'єктів даних.

2. Належні гарантії, вказані в п. 1, можна надавати без запиту на отримання від наглядового органу будь-якого спеціального дозволу:

a) юридично зобов'язальним інструментом, що підлягає застосуванню, між публічними органами чи організаціями;

b) зобов'язальними корпоративними правилами, згідно зі ст. 47;

c) стандартними положеннями щодо захисту даних, ухваленими Комісією відповідно до експертної процедури, зазначеної в ст. 93 (2);

d) стандартними положеннями щодо захисту даних, ухваленими наглядовим органом і затвердженими Комісією відповідно до експертної процедури, зазначеної в ст. 93 (2);

e) затвердженим кодексом поведінки, відповідно до ст. 40, в поєднанні із зобов'язаннями контролера або оператора в третій країні, що підлягають обов'язковому виконанню, щодо вжиття належних гарантій, у тому числі в частині прав суб'єктів даних; або

f) затвердженим механізмом сертифікації, відповідно до ст. 42, в поєднанні із зобов'язаннями контролера або оператора в третій країні, що підлягають обов'язковому виконанню, щодо вжиття належних гарантій, у тому числі в частині прав суб'єктів даних; або

3. З урахуванням дозволу компетентного наглядового органу належні гарантії, вказані в п. 1, можна також надавати, зокрема:

a) положеннями договору між контролером або оператором і контролером, оператором або одержувачем персональних даних у третій країні чи міжнародною організацією; або

b) положеннями, які необхідно включити до адміністративних домовленостей між публічними органами чи організаціями, що містять дієві та можливі для виконання права суб'єкта даних.

4. Наглядовий орган застосовує механізм послідовності, вказаний у ст. 63, у випадках, передбачених у п. 3 цієї статті.

5. Дозволи, надані державою-членом або наглядовим органом на підставі ст. 26 (2) Директиви 95/46/ЄС, залишаються чинними до внесення таким наглядовим органом змін і доповнень, заміни або скасування, за необхідності. Рішення, ухвалені Комісією на підставі ст. 26 (4) Директиви 95/46/ЄС, залишаються чинними до внесення змін чи доповнень, заміни або скасування, за необхідності, Рішенням Комісії, ухваленим згідно з п. 2 цієї статті.

Стаття 47

Зобов'язальні корпоративні правила

1. Компетентний наглядовий орган затверджує зобов'язальні корпоративні правила відповідно до механізму послідовності, викладеного в ст. 63, за умови, що вони:

a) мають обов'язкову юридичну силу, їх застосовує і забезпечує їх виконання кожний зацікавлений член групи підприємств або групи підприємств, що провадять спільну господарську діяльність, в тому числі їхні працівники;

b) прямо надають суб'єктам даних права, які можна реалізувати у зв'язку з опрацюванням їхніх персональних даних; і

c) відповідають вимогам, викладеним у п. 2.

2. Зобов'язальні корпоративні правила, вказані в п. 1, повинні чітко визначати принаймні:

a) структуру та контактні дані групи підприємств або групи підприємств, що провадять спільну господарську діяльність, і кожного з їх членів;

b) передавання даних чи низку актів передавання, у тому числі категорії персональних даних, тип опрацювання і його цілі, тип суб'єктів даних, що зазнали впливу, та визначення відповідної третьої країни чи країн;

c) їх обов'язкову юридичну природу, як внутрішню, так і зовнішню;

d) застосування загальних принципів захисту даних, зокрема, цільове обмеження, мінімізацію даних, обмежені періоди зберігання, якість даних, захист даних за призначенням і за замовчуванням, законодавчу базу опрацювання, опрацювання спеціальних категорій персональних даних, заходи для гарантування безпеки даних і вимоги щодо наступних актів передавання до органів, що не пов'язані зобов'язальними корпоративними правилами;

e) права суб'єктів даних у сфері опрацювання і засоби реалізації таких прав, у тому числі право не підпорядковуватися рішенням, що ґрунтуються винятково на автоматизованому опрацюванні, в тому числі профайлінгу, відповідно до ст. 22, право подавати скаргу до компетентного наглядового органу та компетентних судів держав-членів, згідно зі ст. 79, та отри-

мувати правовий захист і, за необхідності, відшкодування за порушення зобов'язальних корпоративних правил;

f) визнання контролером або оператором, що має осідок на території держави-члена, відповідальності за будь-які порушення зобов'язальних корпоративних правил будь-яким залученим членом, що перебуває поза межами Союзу; контролер або оператор звільняються від такої відповідальності частково або повністю, лише якщо доведено, що такий член не несе відповідальності за подію, внаслідок якої заподіяно шкоду;

g) як інформацію про зобов'язальні корпоративні правила, зокрема про положення, вказані в пп. *d*, *e* і *f* цього параграфа, надають суб'єктам даних, як доповнення до ст. 13 і 14;

h) завдання будь-якого співробітника з питань захисту даних, призначеного відповідно до ст. 37, або будь-якої іншої особи чи установи, відповідальної за моніторинг дотримання зобов'язальних корпоративних правил у межах групи підприємств або групи підприємств, що провадять спільну господарську діяльність, а також моніторинг підготування та розгляду скарг;

i) процедури подання і розгляду скарг;

j) механізми в межах групи підприємств або групи підприємств, що провадять спільну господарську діяльність, для забезпечення перевірки відповідності зобов'язальним корпоративним правилам. Такі механізми передбачають перевірку захисту даних і методів забезпечення вжиття виправних дій для захисту прав суб'єкта даних. Результати такої перевірки необхідно повідомляти особі чи установі, вказаній у пп. *h*, і раді контролюючого підприємства групи підприємств чи групи підприємств, що провадять спільну господарську діяльність, та надавати на запит компетентного наглядового органу;

k) механізми звітування та внесення змін до правил і звітування про такі зміни до наглядового органу;

l) механізм співпраці з наглядовим органом для забезпечення дотримання будь-яким членом групи підприємств або групи підприємств, що провадять спільну господарську діяльність, зокрема шляхом надання наглядовому органу результатів перевірок заходів, вказаних у пп. *j*;

m) механізми для звітування компетентному наглядовому органу про будь-які законні вимоги, які поширюються на члена групи підприємств або групи підприємств, що провадять спільну господарську діяльність у третій країні, що, ймовірно, матимуть суттєві негативні наслідки для гарантій, передбачених зобов'язальними корпоративними правилами; та

n) відповідне навчання з питань захисту даних для персоналу, що має постійний або регулярний доступ до персональних даних.

3. Комісія має право визначити формат і процедури обміну інформацією між контролерами, операторами і наглядовими органами для виконання зобов'язальних корпоративних правил у значенні цієї статті. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, встановленої в ст. 93 (2).

Стаття 48

Передавання або розкриття, не дозволені законодавством Союзу

Будь-яке рішення суду або трибуналу та будь-яке рішення адміністративного органу в третій країні, що вимагає від контролера або оператора передати чи розкрити персональні дані, може бути визнане чи виконане у будь-який спосіб, якщо воно базується на міжнародній угоді, такій як договір про взаємну правову допомогу, яка є чинною для третьої країни, що подає запит, Союзом або державою-членом, без обмеження інших підстав для передавання, відповідно до цієї глави.

Стаття 49

Винятки для спеціальних ситуацій

1. За відсутності рішення про відповідність, згідно зі ст. 45 (3), або належних гарантій, відповідно до ст. 46, в тому числі зобов'язальних корпоративних правил, передавання чи низка актів передавання персональних даних до третьої країни чи міжнародної організації відбувається лише за однієї з таких умов:

a) суб'єкт даних надав чітку згоду на запропоноване передавання після того, як його було повідомлено про можливі

ризики такого передавання для суб'єкта даних, зважаючи на відсутність рішення про відповідність і належних гарантій;

b) передавання є необхідним для виконання контракту між суб'єктом даних і контролером або реалізації переддоговірних заходів, вжитих на запит суб'єкта даних;

c) передавання є необхідним для укладення чи виконання договору, укладеного в інтересах суб'єкта даних між контролером та іншою фізичною чи юридичною особою;

d) передавання є необхідним для задоволення суспільного інтересу;

e) передавання є необхідним для формування, здійснення або захисту правових претензій;

f) передавання є необхідним для захисту життєво важливих інтересів суб'єкта даних або інших осіб, якщо суб'єкт даних фізично чи юридично неспроможний надати згоду;

g) передавання здійснюють з реєстру, що, відповідно до законодавства Союзу або держави- члена, призначений для надання інформації громадськості та є відкритим для доступу як громадськості загалом, так і будь-якої іншої особи, яка може довести законний інтерес, але лише тією мірою, якою в конкретному випадку доступу виконано умови, передбачені законодавством Союзу або держави-члена.

Якщо передавання не можна обґрунтувати на підставі положень ст. 45 чи 46, в тому числі положень про зобов'язальні корпоративні правила, а жодний з винятків, передбачених для спеціальної ситуації, вказаної в п. 1 цього параграфа, не є застосовним, передавання до третьої країни чи до міжнародної організації може відбутися лише у разі, якщо передавання не є повторюваним, стосується лише обмеженої кількості суб'єктів даних, є необхідним для задоволення істотних законних інтересів контролера, над якими не переважають інтереси чи права і свободи суб'єкта даних, і контролер оцінив усі обставини, що супроводжують передавання даних, і на підставі такої оцінки надав належні гарантії щодо захисту персональних даних. Контролер повинен поінформувати наглядовий орган про передавання. Окрім надання інформації, вказаної в ст. 13 і 14, контролер інформує суб'єкта

даних про передавання та свої істотні законні інтереси, які він переслідує.

2. Передавання, відповідно до пп. *g* п. 1, не охоплює всі персональні дані чи всі категорії персональних даних, що містяться в реєстрі. Якщо реєстр призначений для доступу осіб, які мають законний інтерес, передавання здійснюють лише на запит таких осіб, або якщо вони мають бути одержувачами.

3. Пункти *a*, *b* і *c* пп. 1 та пп. 2 п. 1 не застосовують до видів діяльності, які провадять органи публічної влади під час виконання своїх публічних повноважень.

4. Суспільний інтерес, вказаний в пп. *d* п. 1, визнається законодавством Союзу чи законодавством держави-члена, яке поширюється на контролера.

5. За відсутності рішення про відповідність законодавство Союзу або держави-члена можуть, на важливих підставах суспільного інтересу, чітко встановлювати обмеження на передавання спеціальних категорій даних до третьої країни чи міжнародної організації. Держави-члени повідомляють Комісію про такі положення.

6. Контролер або оператор повинні задокументувати оцінку, а також належні гарантії, вказані в пп. 2 п. 1 цієї статті, у формі записів, вказаних у ст. 30.

Стаття 50

Міжнародна співпраця у сфері захисту персональних даних

У тому, що стосується третіх країн і міжнародних організацій, Комісія та наглядові органи вживають необхідних заходів для:

a) розвитку механізмів міжнародної співпраці з метою сприяння ефективному застосуванню законодавства з метою захисту персональних даних;

b) надання міжнародної взаємної допомоги в застосуванні законодавства з метою захисту персональних даних, у тому числі через повідомлення, подання скарг, допомогу в проведенні розслідувань та обмін інформацією з урахуванням необхідних гарантій для захисту персональних даних та інших фундаментальних прав і свобод;

c) залучення відповідних стейкхолдерів до обговорення та діяльності, спрямованої на розвиток міжнародної співпраці щодо застосування законодавства з метою захисту персональних даних;

d) сприяння обміну документацією та практикою захисту персональних даних, у тому числі щодо юрисдикційних колізій з третіми країнами.

Розділ VI. Незалежні наглядові органи

Секція 1

Незалежний статус

Стаття 51

Наглядовий орган

1. Кожна держава-член покладає на один або декілька незалежних публічних органів відповідальність за моніторинг застосування цього Регламенту для того, щоб захистити фундаментальні права та свободи фізичних осіб у сфері опрацювання та сприяти вільному переміщенню персональних даних у межах Союзу («наглядовий орган»).

2. Кожний наглядовий орган сприяє послідовному застосуванню цього Регламенту в межах Союзу. З цією метою наглядові органи співпрацюють один з одним і з Комісією, відповідно до глави VII.

3. Якщо в державі-члені створено більше аніж один наглядовий орган, така держава-член призначає наглядовий орган, який представлятиме такі органи в Раді, та встановлює механізм забезпечення дотримання іншими органами правил щодо механізму послідовності, вказаного в ст. 63.

4. Кожна держава-член повідомляє Комісію про положення свого закону, який вона ухвалює відповідно до цієї глави, до 25 травня 2018 р. та, без затримки, про будь-які подальші зміни і доповнення, що на них впливають.

Стаття 52

Незалежність

1. Кожний наглядовий орган діє абсолютно незалежно під час виконання своїх завдань і здійснення своїх повноважень згідно з цим Регламентом.

2. Член або члени кожного наглядового органу під час виконання своїх завдань і здійснення своїх повноважень згідно з цим Регламентом повинні залишатися вільними від зовнішнього впливу, прямого чи опосередкованого, та не повинні запитувати чи приймати вказівки від будь-якої особи.

3. Член або члени кожного наглядового органу повинні утримуватися від будь-яких дій, що суперечать їхнім обов'язкам, та не повинні, протягом строку їхніх повноважень, провадити будь-яку несумісну діяльність, прибуткову чи ні.

4. Кожна держава-член забезпечує, щоб усі наглядові органи мали у своєму розпорядженні людські, технічні та фінансові ресурси, приміщення та інфраструктуру, необхідні для результативного виконання їхніх завдань та здійснення повноважень, у тому числі в контексті взаємної допомоги, співпраці та участі в Раді.

5. Кожна держава-член забезпечує, щоб усі наглядові органи обирали і мали свій власний персонал, безпосередньо підпорядкований відповідному члену чи членам наглядового органу.

6. Кожна держава-член забезпечує, щоб усі наглядові органи підлягали фінансовому контролю, що не порушує його незалежності, і мали окремі публічні річні бюджети, що можуть бути частиною загальнодержавного чи національного бюджету.

Стаття 53

Загальні умови для членів наглядового органу

1. Держави-члени забезпечують, щоб кожен член їх наглядових органів був призначений у порядку прозорої процедури:

– їх парламент;

– їх уряд;

– їх голова держави; або

– незалежний орган, якому доручено здійснити призначення, згідно з законодавством держави-члена.

2. Кожен член повинен мати кваліфікацію, досвід і вміння, зокрема, в сфері захисту персональних даних, необхідні для виконання його обов'язків і здійснення повноважень.

3. Обов'язки члена припиняються в разі закінчення строку повноваження, відставки чи обов'язкового виходу на пенсію, згідно з законодавством відповідної держави-члена.

4. Член підлягає звільненню, лише якщо він вчинив серйозний проступок або не виконує своїх обов'язків.

Стаття 54

Правила заснування наглядового органу

1. Кожна держава-член на законодавчому рівні повинна визначити:

a) процедуру заснування кожного наглядового органу;

b) вимоги до кваліфікації та умови прийнятності, необхідні для призначення членів наглядового органу;

c) правила і процедури призначення членів наглядового органу;

d) тривалість строку повноважень членів наглядового органу становить не менше чотирьох років, за винятком першого призначення, після 24 травня 2016 р., частина якого може становити коротший період, якщо це необхідно для захисту незалежності наглядового органу за допомогою поетапної процедури призначення;

e) чи і, якщо так, на скільки строків можна повторно призначити члена чи членів наглядового органу;

f) умови, що регулюють обов'язки членів і персоналу наглядового органу, заборони на дії, види діяльності та переваги, несумісні з ними, протягом і після строку повноважень і правила, що регулюють припинення зайнятості.

2. На члена або членів і персонал наглядового органу поширюється, згідно з законодавством Союзу або держави-члена, обов'язок збереження професійної таємниці як протягом, так і після строку їх повноважень, щодо будь-якої конфіденційної інформації, про яку вони дізналися під час

виконання своїх завдань або реалізації своїх повноважень. Під час строку їх повноважень обов'язок збереження професійної таємниці, зокрема, застосовують при звітуванні фізичних осіб про порушення за цим Регламентом.

Секція 2

Компетенція, завдання і повноваження

Стаття 55

Компетенція

1. Кожен наглядовий орган має компетенцію для виконання завдань і реалізації повноважень, покладених на нього згідно з цим Регламентом на території його власної держави-члена.

2. Якщо опрацювання здійснюють публічні органи або приватні органи, які діють на підставі пп. *c* або *e* ст. 6 (1), компетенцію має наглядовий орган відповідної держави-члена. У таких випадках ст. 56 не застосовують.

3. Наглядові органи не мають компетенції провадити нагляд за операціями опрацювання, які здійснюють суди, що діють як судові інстанції.

Стаття 56

Компетенція керівного наглядового органу

1. Без обмеження ст. 55 наглядовий орган за головним осідком або єдиним осідком контролера або оператора має компетенцію діяти як керівний наглядовий орган для транскордонного опрацювання, яке здійснює контролер або оператор відповідно до процедури, передбаченої ст. 60.

2. Відступаючи від п. 1, кожен наглядовий орган має компетенцію розглядати скаргу, подану до нього, або можливе порушення положень цього Регламенту, якщо предмет стосується лише осідку в його державі-члені чи істотно впливає на суб'єктів даних лише в його державі-члені.

3. У випадках, передбачених у п. 2 цієї статті, наглядовий орган повідомляє керівний наглядовий орган про такі питання без затримки. Протягом тритижневого періоду від дати отримання повідомлення керівний наглядовий орган

повинен вирішити, чи розглядатиме справу згідно з процедурою, передбаченою ст. 60, зважаючи на те, чи осідок контролера або оператора знаходиться в державі-члені, з якої наглядовий орган повідомив про це.

4. Якщо керівний наглядовий орган вирішує розглядати справу, застосовують процедуру, передбачену ст. 60. Наглядовий орган, який повідомив керівний наглядовий орган, може подати керівному наглядовому органу проект рішення. Керівний наглядовий орган звертає максимальну увагу на такий проект під час підготування проекту рішення, вказаного в ст. 60 (3).

5. Якщо наглядовий орган вирішує не розглядати справу, наглядовий орган, який повідомив керівний наглядовий орган, повинен розглянути її відповідно до ст. 61 і 62.

6. Керівний наглядовий орган є єдиним посередником контролера або оператора в транскордонному опрацюванні, яке вони здійснюють.

Стаття 57

Завдання

1. Без обмеження інших завдань, передбачених цим Регламентом, кожен наглядовий орган на своїй території:

a) здійснює моніторинг і забезпечує застосування цього Регламенту;

b) сприяє обізнаності громадськості та її розумінню ризиків, правил, гарантій і прав у зв'язку з опрацюванням. Особливої уваги потребує опрацювання, спрямоване безпосередньо на дітей;

c) консультує, згідно з законодавством держави-члена, національний парламент, уряд та інші установи й органи щодо законодавчих і адміністративних інструментів, пов'язаних із захистом прав і свобод фізичних осіб в процесі опрацювання;

d) сприяє обізнаності контролерів і операторів про їхні обов'язки за цим Регламентом;

e) на запит надає інформацію будь-якому суб'єкту даних щодо реалізації його прав за цим Регламентом і, за необхідності, з цією метою співпрацює з наглядовими органами в інших державах-членах;

f) розглядає скарги, подані суб'єктом даних або органом, організацією чи асоціацією, згідно зі ст. 80, і розслідує, наскільки це можливо, предмет скарги та інформує позивача про перебіг і наслідки розслідування в розумний строк, зокрема якщо існує необхідність подальшого розслідування чи координації з іншим наглядовим органом;

g) співпрацює, в тому числі шляхом обміну інформацією та надання взаємної допомоги, з іншими наглядовими органами для забезпечення послідовності застосування та виконання цього Регламенту;

h) провадить розслідування щодо застосування цього Регламенту, в тому числі на підставі інформації, отриманої від іншого наглядового органу чи іншого публічного органу;

i) здійснює моніторинг відповідних тенденцій, доки вони впливають на захист персональних даних, зокрема розроблення інформаційно-комунікаційних технологій і комерційної практики;

j) ухвалює стандартні договірні положення, згадані в ст. 28 (8) та пп. *d* ст. 46 (2);

k) започатковує і веде список, відповідно до вимог щодо оцінювання впливу на захист даних, згідно зі ст. 35 (4);

l) консультує щодо операцій опрацювання, вказаних у ст. 36 (2);

m) заохочує розроблення кодексів поведінки, відповідно до ст. 40 (1), надає висновок і схвалює кодекси поведінки, що забезпечують достатні гарантії, відповідно до ст. 40 (5);

n) заохочує запровадження механізмів сертифікації захисту даних, штампів і знаків захисту даних, згідно зі ст. 42 (1), і схвалює критерії сертифікації, згідно зі ст. 42 (5);

o) за необхідності, здійснює періодичний перегляд сертифікатів, виданих згідно зі ст. 42 (7);

p) розробляє та публікує критерії для акредитації органу з моніторингу кодексів поведінки, згідно зі ст. 41, чи органу сертифікації, згідно зі ст. 43;

q) провадить акредитацію органу з моніторингу кодексів поведінки, згідно зі ст. 41, чи органу сертифікації, згідно зі ст. 43;

r) надає дозвіл на договірні положення, вказані в ст. 46 (3);

s) ухвалює зобов'язальні корпоративні правила, відповідно до ст. 47;

t) сприяє діяльності Ради;

u) веде внутрішні записи порушень положень цього Регламенту та заходів, вжитих згідно зі ст. 58(2); і

v) виконує будь-які інші завдання, пов'язані з захистом персональних даних.

2. Кожен наглядовий орган спрощує процедуру подання скарг, вказаних у пп. *f* п. 1, за допомогою таких заходів, як форма подання скарги, яку також можна оформити в електронному форматі без обмеження інших засобів зв'язку.

3. Свої завдання наглядові органи виконують на безоплатній основі для суб'єкта даних і, за необхідності, для співробітника з питань захисту даних.

4. Якщо запити є явно необґрунтованими чи надмірними, зокрема через їх багаторазове повторення, наглядовий орган може стягувати розумну плату, що ґрунтується на адміністративних витратах, або ухилитися від виконання дій у відповідь на запит. Наглядовий орган повинен нести тягар доведення явно необґрунтованого чи надмірного характеру запиту.

Стаття 58

Повноваження

1. Кожен наглядовий орган має всі слідчі повноваження, а саме:

a) видавати розпорядження контролеру або оператору і, за необхідності, представнику контролера або оператора надати будь-яку інформацію, якої він потребує для виконання своїх завдань;

b) провадити розслідування в формі перевірок захисту даних;

c) здійснювати перегляд сертифікатів, виданих згідно зі ст. 42 (7);

d) повідомляти контролера або оператора про передбачуване порушення цього Регламенту;

e) отримувати, від контролера або оператора, доступ до всіх персональних даних і до всієї інформації, необхідної для виконання його завдань;

f) отримувати доступ до будь-яких приміщень контролера або оператора, в тому числі до будь-якого обладнання і засобів опрацювання даних, згідно з процесуальним законодавством Союзу чи держави-члена.

2. Кожен наглядовий орган має всі виправні повноваження, а саме:

a) надсилати попередження контролеру або оператору про те, що призначені операції опрацювання ймовірно суперечитимуть положенням цього Регламенту;

b) виносити догану контролеру або оператору, якщо операції опрацювання порушують положення цього Регламенту;

c) наказувати контролеру або оператору дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до цього Регламенту;

d) наказувати контролеру або оператору узгодити операції опрацювання з положеннями цього Регламенту, за необхідності, у встановленому порядку та протягом встановленого періоду;

e) наказувати контролеру повідомити суб'єкта даних про порушення захисту персональних даних;

f) накладати тимчасове чи остаточне обмеження, в тому числі заборону, на опрацювання;

g) наказувати внести виправлення чи вилучити персональні дані або обмежити опрацювання, згідно зі ст. 16, 17 і 18, і повідомити про такі дії кожного одержувача, персональні дані якого було розкрито, відповідно до ст. 17 (2) і ст. 19;

h) відкликати сертифікат чи наказати органу сертифікації відкликати сертифікат, виданий відповідно до ст. 42 і 43, або наказати органу сертифікації не видавати сертифікат, якщо вимоги для сертифікації не виконано або більше не виконуються;

i) накладати адміністративні штрафи, відповідно до ст. 83, як доповнення до заходів, чи замість заходів, вказаних у цьому пункті, залежно від обставин кожної індивідуальної справи;

j) наказувати призупинити потоки даних до одержувача в третій країні чи до міжнародної організації.

3. Кожен наглядовий орган має всі дозвільні і консультативні повноваження, а саме:

a) консультувати контролера відповідно до процедури попередніх консультацій, вказаної в ст. 36;

b) надавати, з власної ініціативи чи на запит, для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості висновки щодо будь-якого питання, пов'язаного з захистом персональних даних;

c) надавати дозвіл на опрацювання, вказане в ст. 36 (5), якщо законодавство держави-члена вимагає надання такого попереднього дозволу;

d) надавати висновок і затверджувати проекти кодексів поведінки, відповідно до ст. 40 (5);

e) надавати акредитацію органам сертифікації, відповідно до ст. 43;

f) видавати сертифікати та затверджувати критерії сертифікації, відповідно до ст. 42 (5);

g) ухвалювати стандартні положення щодо захисту даних, вказані в ст. 28 (8) та пп. *d* ст. 46 (2);

h) надавати дозвіл на договірні положення, вказані в пп. *a* ст. 46 (3);

i) надавати дозвіл на адміністративні домовленості, вказані в пп. *b* ст. 46 (3);

j) затверджувати зобов'язальні корпоративні правила, відповідно до ст. 47.

4. На реалізацію повноважень, покладених на наглядовий орган відповідно до цієї статті, поширюються належні гарантії, у тому числі дієвий судовий засіб правового захисту та належний процес, передбачений законодавством Союзу або держави-члена, згідно з Хартією.

5. Кожна держава-член забезпечує на законодавчому рівні, щоб її наглядовий орган було наділено повноваженням повідомляти про порушення цього Регламенту судові органи

і, в разі необхідності, розпочинати процесуальні дії чи іншим чином залучати до них для того, щоб забезпечити виконання положень цього Регламенту.

6. Кожна держава-член може передбачити на законодавчому рівні, щоб її наглядовий орган було наділено додатковими повноваженнями, крім тих, що вказані в п. 1, 2 і 3. Реалізація таких повноважень не повинна перешкоджати результативному застосуванню розділу VII.

Стаття 59

Звіти про виконану роботу

Кожен наглядовий орган складає щорічний звіт про свою діяльність, що може містити перелік порушень, про які було повідомлено, та заходів, яких було вжито, відповідно до ст. 58 (2). Ці звіти передають до національного парламенту, уряду та інших органів, як це передбачено законодавством держави-члена. Громадськість, Комісія та Рада отримують до них доступ.

Розділ VII. Співпраця і послідовність

Секція 1

Співпраця

Стаття 60

Співпраця між керівним наглядовим органом та іншими відповідними наглядовими органами

1. Керівний наглядовий орган співпрацює з іншими наглядовими органами, відповідно до цієї статті, прагнучи досягти консенсусу. Керівний наглядовий орган і відповідні наглядові органи обмінюються всією належною інформацією.

2. Керівний наглядовий орган може надсилати запит у будь-який час до інших наглядових органів на надання взаємної допомоги відповідно до ст. 61, і може організовувати спільні операції, відповідно до ст. 62, зокрема, для провадження розслідувань або для моніторингу реалізації заходу щодо контролера або оператора, що має осідок в іншій державі-члені.

3. Керівний наглядовий орган повинен, без затримки, повідомити відповідну інформацію щодо питання іншим наг-

лядовим органам. Він повинен без затримки надіслати проект рішення іншим наглядовим органам для отримання їх висновку та належним чином врахувати їх думки.

4. Якщо будь-який з інших наглядових органів протягом чотирьох тижнів після отримання консультації, згідно з п. 3 цієї статті, висловлює належне та обґрунтоване заперечення щодо проекту рішення, керівний наглядовий орган повинен, якщо він не зважає на відповідне обґрунтоване заперечення або якщо вважає, що заперечення не є належним чином обґрунтованим, передати питання до механізму послідовності, вказаному в ст. 63.

5. Якщо керівний наглядовий орган має намір враховувати висловлене належне та вмотивоване заперечення, він повинен надати іншим наглядовим органам допрацьований проект рішення для отримання їх висновку. Допрацьований проект рішення підлягає процедурі, описаний у п. 4, протягом двотижневого терміну.

6. Якщо жоден з наглядових органів не має заперечень щодо проекту рішення, поданого керівним наглядовим органом, протягом періоду, вказаного в п. 4 і 5, керівний наглядовий орган і відповідні наглядові органи можна вважати такими, що погоджуються із таким проектом рішення і зобов'язані ним.

7. Керівний наглядовий орган ухвалює рішення і повідомляє про нього до головного чи єдиного осідку контролера або оператора, залежно від обставин, і повідомляє інші відповідні наглядові органи та Раду про рішення, що розглядається, в тому числі про належні факти та підстави. Наглядовий орган, до якого подано скаргу, повідомляє позивача про рішення.

8. Відступаючи від п. 7, якщо скаргу відхилено чи у ній відмовлено, наглядовий орган, до якого подано скаргу, ухвалює рішення та повідомляє про нього позивача та контролера.

9. Якщо керівний наглядовий орган і відповідні наглядові органи погоджуються відхилити або відмовити в частині скарги та діяти щодо інших частин такої скарги, окреме рішення ухвалюють для кожної такої частини справи. Керівний наглядовий орган ухвалює рішення щодо частини, що стосується оператора,

повідомляє про це головний чи єдиний осідок контролера або оператора на території своєї держави-члена та повідомляє про це позивача, водночас наглядовий орган позивача ухвалює рішення щодо частини, яка стосується відхилення чи відмови в такій заяві, та повідомляє про це такому позивачу й інформує про це контролера або оператора.

10. Отримавши повідомлення про рішення керівного наглядового органу, відповідно до п. 7 і 9, контролер або оператор вживають необхідних заходів для виконання рішення в частині, що стосується опрацювання даних у контексті всіх його осідків у Союзі. Контролер або оператор повідомляють про заходи, вжиті для виконання рішення, керівному наглядовому органу, який інформує інші відповідні наглядові органи.

11. Якщо, за виняткових обставин, відповідний наглядовий орган має підстави вважати, що існує нагальна потреба вживати заходів для захисту інтересів суб'єктів даних, застосовують екстрену процедуру, описану в ст. 66.

12. Керівний наглядовий орган та інші наглядові органи надають інформацію, необхідну за цією статтею, один одному електронними засобами, з використанням стандартного формату.

Стаття 61

Взаємна допомога

1. Наглядові органи надають один одному відповідну інформацію і взаємну допомогу з метою імплементації та послідовного застосування цього Регламенту та вживають заходів для результативної співпраці. Взаємна допомога охоплює, зокрема, інформаційні запити та заходи з нагляду, такі як запити на видачу попередніх дозволів і проведення попередніх консультацій, інспекцій і розслідувань.

2. Кожен наглядовий орган вживає всіх заходів, необхідних для того, щоб відповісти на запит іншого наглядового органу без необґрунтованої затримки та не пізніше одного місяця після отримання запиту. Такі заходи можуть включати, зокрема, передавання інформації про перебіг розслідування.

3. Запити на надання допомоги містять усю необхідну інформацію, в тому числі про цілі та причини запиту. Інформацію, якою обмінюються, необхідно використовувати лише відповідно до цілі, для якої подано запит.

4. Наглядовий орган, до якого надійшов запит, не повинен відмовляти в задоволенні запиту, за винятком тих випадків, коли:

a) він володіє компетенцією щодо предмета запиту чи заходів, на вжиття яких надіслано запит; або

b) задоволення запиту може суперечити положенням цього Регламенту або законодавства Союзу чи держави-члена, яке поширюється на наглядовий орган, до якого надійшов запит.

5. Наглядовий орган, до якого надійшов запит, повідомляє наглядовий орган, який надіслав запит, про результати чи, залежно від обставин, перебіг заходів, вжитих як відповідь на запит. Наглядовий орган, до якого надійшов запит, повинен надати інформацію про причини будь-якої відмови в задоволенні запиту, відповідно до п. 4.

6. Наглядові органи, які отримали запити, як правило, надають інформацію, про яку запитують інші наглядові органи, електронними засобами, з використанням стандартного формату.

7. Наглядові органи, яким надійшли запити, не стягують плати за жодні дії, які вони вчиняють згідно із запитом на взаємну допомогу. Наглядові органи можуть узгоджувати правила відшкодування один одному окремих витрат, що випливають з надання взаємної допомоги за виняткових обставин.

8. Якщо наглядовий орган не надає інформацію, передбачену п. 5 цієї статті, протягом одного місяця з дати отримання запиту від іншого наглядового органу, наглядовий орган, який надіслав запит, може вжити тимчасового заходу на території своєї держави-члена, згідно зі ст. 55 (1). У такому разі передбачається, що негайну потребу діяти, згідно зі ст. 66 (1), задоволено, що вимагає ухвалення негайного зобов'язального рішення Ради, згідно зі ст. 66 (2).

9. Комісія може, шляхом ухвалення імплементаційних актів, визначити формат і процедури взаємної допомоги, вка-

заної в цій статті, та домовленості для обміну інформацією електронними засобами між наглядовими органами та між наглядовими органами і Радою, зокрема стандартний формат, вказаний у п. 6 цієї статті. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, описаної в ст. 93 (2).

Стаття 62

Спільні операції наглядових органів

1. Наглядові органи проводять, за необхідності, спільні операції, в тому числі спільні розслідування і спільні заходи із забезпечення виконання, до яких залучають членів чи персонал наглядових органів інших держав-членів.

2. Якщо контролер або оператор мають осідки в декількох державах-членах або якщо істотна кількість суб'єктів даних у декількох державах-членах ймовірно зазнає істотного впливу внаслідок операцій опрацювання, наглядовий орган кожної з цих держав-членів має право брати участь у спільних операціях. Наглядовий орган, що володіє компетенцією, згідно зі ст. 56 (1) або (4), запрошує наглядовий орган кожної з таких держав-членів до участі в спільних операціях і відповідає без затримки на запит щодо участі від наглядового органу.

3. Наглядовий орган може, згідно із законом держави-члена та з дозволу наглядового органу, що надсилає, надавати повноваження, в тому числі слідчі повноваження, членам або персоналу наглядового органу, що надсилає, залученим до спільних операцій чи, мірою, якою це дозволено законодавством держави-члени за місцем перебування наглядового органу, дозволяти членам чи персоналу наглядового органу, що надсилає, реалізовувати їх слідчі повноваження, згідно з законодавством держави-члена наглядового органу, що надсилає. Такі слідчі повноваження можна здійснювати лише під керівництвом і за присутності членів або персоналу наглядового органу за місцем перебування. Члени або персонал наглядового органу, що надсилає, підпорядковуються законодавству держави-члена наглядового органу за місцем перебування.

4. Якщо, згідно з п. 1, персонал наглядового органу, що надсилає, діє в іншій державі-члені, держава-член за місцем

перебування наглядового органу бере на себе відповідальність за їхні дії, в тому числі за будь-яку шкоду, заподіяну ними під час їхніх операцій, відповідно до законодавства держави-члена, на території якої вони провадять діяльність.

5. Держава-член, на території якої заподіяно шкоду, виправляє її на умовах, які застосовують до шкоди, заподіяної її власним персоналом. Держава-член наглядового органу, що надсилає, чий персонал заподіяв шкоду будь-якій особі на території іншої держави-члена, відшкодовує тій іншій державі-члену повністю будь-які кошти, які вона виплатила особам, що мають на це право, від їхнього імені.

6. Без обмеження реалізації своїх прав щодо третіх сторін і за винятком п. 5, кожна держава-член повинна утримуватися у ситуації, передбаченій п. 1, від вимоги відшкодування від іншої держави-члена шкоди, вказаної в п. 4.

7. Якщо призначено спільну операцію і наглядовий орган протягом одного місяця не дотримується обов'язку, викладеного в другому реченні п. 2 цієї статті, інші наглядові органи можуть вжити тимчасового заходу на території своєї держави-члена, згідно зі ст. 55. У такому разі передбачається, що негайну потребу діяти згідно зі ст. 66 (1) задоволено, що вимагає винесення висновку або ухвалення негайного зобов'язального рішення Ради, згідно зі ст. 66 (2).

Секція 2

Послідовність

Стаття 63

Механізм послідовності

Щоб сприяти послідовному застосуванню цього Регламенту в межах Союзу, наглядові органи повинні співпрацювати один з одним і, в належних випадках, з Комісією, через механізм послідовності, як встановлено в цій секції.

Стаття 64

Висновок Ради

1. Рада ухвалює висновок, на підставі якого компетентний наглядовий орган може ухвалити будь-який з інструментів,

перелічених далі. З цією метою компетентний наглядовий орган повідомляє про проект рішення Ради, якщо воно:

a) спрямоване на ухвалення списку операцій опрацювання з урахуванням вимог до оцінювання впливу на захист даних, згідно зі ст. 35 (4);

b) стосується питання, відповідно до ст. 40 (7), про те, чи відповідає проект кодексу поведінки чи зміни або розширення кодексу поведінки цьому Регламенту;

c) спрямоване на затвердження критеріїв для акредитації органу, згідно зі ст. 41 (3), чи органу сертифікації, згідно зі ст. 43 (3);

d) спрямоване на визначення стандартних положень про захист даних, вказаних у пп. *d* ст. 46 (2) та в ст. 28 (8);

e) спрямоване на надання дозволу на договірні положення, вказані в пп. *a* ст. 46 (3);

чи

f) спрямоване на ухвалення зобов'язальних корпоративних правил у значенні ст. 47.

2. Будь-який наглядовий орган, Голова Ради чи Комісія можуть надіслати запит про те, щоб будь-яке питання загального застосування або таке, що породжує наслідки у декількох державах-членах, було розглянуто Радою, з метою отримання висновку, зокрема, якщо компетентний наглядовий орган не виконує обов'язків щодо взаємної допомоги, згідно зі ст. 61, або щодо спільних операцій, згідно зі ст. 62.

3. У випадках, вказаних у п. 1 і 2, Рада ухвалює висновок з питання, поданого до неї, за умови, що вона не ухвалила висновок з того самого питання раніше. Такий висновок ухвалюють протягом восьми тижнів простою більшістю голосів членів Ради. Цей період може бути подовжено ще на шість тижнів, враховуючи складність предмета. Стосовно проекту рішення, вказаного в п. 1, яке розіслано членам Ради, відповідно до п. 5, члена, який не заперечує протягом розумного строку, визначеного Головою, можна вважати таким, що погодився з проектом рішення.

4. Наглядові органи і Комісія, без необґрунтованої затримки, повідомляють Раді за допомогою електронних засо-

бів, з використанням стандартного формату будь-яку належну інформацію, в тому числі, залежно від обставин, короткий виклад фактів, проект рішення, підстави вжиття такого заходу, та позиції інших наглядових органів.

5. Голова Ради, без необґрунтованої затримки, інформує за допомогою електронних засобів:

a) членів Ради і Комісію про будь-яку інформацію, повідомлену йому з використанням стандартного формату. Секретаріат Ради, в разі необхідності, надає переклади належної інформації; та

b) наглядовий орган, залежно від ситуації, як вказано в п. 1 і 2, і Комісію про висновок й оприлюднює його.

6. Компетентний наглядовий орган не ухвалює свій проект рішення, передбачений в п. 1, протягом періоду, вказаного в п. 3.

7. Наглядовий орган, вказаний у п. 1, повинен належним чином враховувати висновок Ради та, протягом двох тижнів з дати отримання висновку, повідомляти Голову Ради за допомогою електронних засобів про те, чи залишає він без змін або чи вносить зміни та доповнення до її проекту рішення і, якщо такі будуть, проект рішення з внесеними змінами та доповненнями, з використанням стандартного формату.

8. Якщо відповідний наглядовий орган інформує Голову Ради протягом періоду, вказаного в п. 7 цієї статті, що не має наміру враховувати висновок Ради, загалом чи частково, обґрунтувавши відповідні підстави, у такому разі застосовують ст. 65 (1).

Стаття 65

Урегулювання спорів Радою

1. Щоб забезпечити точне і послідовне застосування цього Регламенту в окремих випадках, Рада ухвалює зобов'язальне рішення для таких випадків:

a) якщо в ситуації, вказаній у ст. 60 (4), відповідний наглядовий орган висунув належне і обґрунтоване заперечення щодо проекту рішення керівного органу або якщо керівний орган відхилив таке заперечення як неналежне чи необґрун-

товане. Зобов'язальне рішення стосується всіх питань, що є предметом належного та обґрунтованого заперечення, зокрема того, чи було порушено цей Регламент;

b) у разі виникнення розбіжностей щодо того, який із відповідних наглядових органів є компетентним для цілей головного осідку;

c) якщо компетентний наглядовий орган не запитує висновку Ради у ситуаціях, передбачених ст. 64 (1), або не враховує висновку Ради, ухваленого згідно зі ст. 64. У такому разі будь-який відповідний наглядовий орган або Комісія може передати питання на розгляд Раді.

2. Рішення, зазначене в п. 1, ухвалюють протягом одного місяця від дати направлення предмета більшістю в дві третини голосів членів Ради. Цей період може бути подовжено ще на місяць, враховуючи складність питання. Рішення, вказане в п. 1, повинно бути вмотивованим й адресованим керівному наглядовому органу та всім відповідним наглядовим органам і бути зобов'язальним для них.

3. Якщо Рада не змогла ухвалити рішення протягом періодів, вказаних у п. 2, вона повинна ухвалити своє рішення протягом двох тижнів після закінчення другого місяця, вказаного в п. 2, простою більшістю голосів членів Ради. У разі виникнення розбіжностей серед членів Ради, рішення ухвалює Голова.

4. Відповідні наглядові органи не повинні ухвалювати рішення щодо питання, поданого на розгляд до Ради, згідно з п. 1, протягом періодів, вказаних у *п.* 2 і 3.

5. Голова Ради повідомляє, без необґрунтованої затримки, про рішення, згадане в п. 1, відповідні наглядові органи. Він інформує про це Комісію. Рішення публікують на сторінці Ради в мережі Інтернет без затримки після того, як наглядовий орган повідомив остаточне рішення, зазначене в п. 6.

6. Керівний наглядовий орган або, залежно від ситуації, наглядовий орган, до якого подано скаргу, ухвалює своє остаточне рішення на підставі рішення, вказаного в п. 1 цієї статті, без необґрунтованої затримки та щонайменше протягом одного місяця після того, як Рада повідомила про своє рішення. Керів-

ний наглядовий орган або, залежно від ситуації, наглядовий орган, до якого подано скаргу, інформує Раду про дату, коли про його остаточне рішення повідомлено, відповідно, контролеру або оператору та суб'єкту даних. Остаточне рішення відповідних наглядових органів ухвалюють на умовах ст. 60 (7), (8) і (9). Остаточне рішення повинно базуватися на рішенні, вказаному в п. 1 цієї статті, та уточнювати, що рішення, згадане в цьому пункті, буде опубліковано на сторінці Ради в мережі Інтернет, відповідно до п. 5 цієї статті. Остаточне рішення додають до рішення, вказаного в п. 1 цієї статті.

Стаття 66

Екстрена процедура

1. За виняткових обставин, якщо залучений наглядовий орган вважає, що існує нагальна потреба вжити заходів для захисту інтересів суб'єктів даних, він може, шляхом застосування винятків з механізму послідовності, описаного в ст. 63, 64 і 65, або процедури, викладеної в ст. 60, негайно вжити тимчасових заходів, спрямованих на породження юридичних наслідків на своїй території з уточненим строком дійсності, що не перевищує трьох місяців. Наглядовий орган повинен, без затримки, повідомити про такі заходи та причини їх вжиття іншим відповідним наглядовим органам, Раді та Комісії.

2. Якщо наглядовий орган вжив захід, відповідно до п. 1, та вважає, що необхідно негайно ухвалити остаточні інструменти, він може надіслати запит на отримання від Ради термінового висновку чи ухвалення термінового зобов'язального рішення, надаючи інформацію про підстави запиту на такий висновок чи рішення.

3. Будь-який наглядовий орган може надсилати запит на отримання від Ради термінового висновку чи ухвалення термінового зобов'язального рішення, залежно від обставин, якщо компетентний наглядовий орган не вжив необхідного заходу в ситуації, де існує нагальна потреба діяти, щоб захистити права та свободи суб'єктів даних, надаючи інформацію про підстави для запиту на такий висновок чи рішення, в тому числі для нагальної потреби діяти.

4. Відступаючи від ст. 64 (3) і ст. 65 (2), терміновий висновок чи термінове зобов'язальне рішення, вказані в п. 2 і 3 цієї статті, ухвалюють протягом двох тижнів простою більшістю голосів членів Ради.

Стаття 67

Обмін інформацією

Комісія може ухвалювати імплементаційні акти загальної сфери дії для того, щоб визначити домовленості щодо обміну інформацією електронними засобами між наглядовими органами та між наглядовими органами і Радою, зокрема, стандартний формат, вказаний у ст. 64.

Такі імплементаційні акти ухвалюють відповідно до експертної процедури, описаної в ст. 93 (2).

Секція 3

Європейська рада із захисту даних

Стаття 68

Європейська рада із захисту даних

1. Цим створюється Європейська рада із захисту даних («Рада») як орган Союзу, що має правосуб'єктність.

2. Раду представляє її Голова.

3. Рада складається з голови одного наглядового органу кожної держави-члена та Європейського інспектора із захисту даних або їх відповідних представників.

4. Якщо в державі-члені більше ніж один наглядовий орган несе відповідальність за моніторинг застосування положень цього Регламенту, призначають спільного представника, відповідно до права держави-члена.

5. Комісія має право брати участь у роботі та засіданнях Ради без права голосу. Комісія призначає представника. Голова Ради повідомляє Комісії про роботу Ради.

6. У випадках, передбачених ст. 65, Європейський інспектор із захисту даних має право голосу лише щодо рішень, які стосуються принципів і правил, застосовних до установ, органів, служб і агентств Союзу, які за суттю відповідають принципам і нормам цього Регламенту.

Стаття 69

Незалежність

1. Рада діє незалежно під час виконання своїх завдань чи здійснення своїх повноважень, відповідно до ст. 70 і 71.

2. Без обмеження запитів Комісії, вказаних у пп. *b* ст. 70 (1) та ст. 70 (2), Рада, під час виконання своїх завдань чи здійснення своїх повноважень, не повинна запитувати чи приймати вказівки від будь-якої особи.

Стаття 70

Завдання Ради

1. Рада забезпечує послідовне застосування цього Регламенту. З цією метою Рада, з власної ініціативи або, за необхідності, на запит Комісії, зокрема:

a) здійснює моніторинг і забезпечує правильне застосування цього Регламенту у випадках, передбачених ст. 64 і 65, без обмеження завдань національних наглядових органів;

b) консультує Комісію з будь-якого питання, пов'язаного з захистом персональних даних у Союзі, в тому числі щодо будь-яких змін і доповнень, які запропоновано внести до цього Регламенту;

c) консультує Комісію щодо формату і процедур для обміну інформацією між контролерами, операторами та наглядовими органами про зобов'язальні корпоративні правила;

d) видає настанови, рекомендації та інформацію про досвід застосування процедур з вилучення посилань, копій чи накладів персональних даних із загальнодоступних послуг зв'язку, вказаних у ст. 17 (2);

e) розглядає, з власної ініціативи, на запит одного з її членів або на запит Комісії, будь-яке питання, що стосується застосування цього Регламенту та видає настанови, рекомендації та інформацію про досвід застосування для того, щоб заохотити до послідовного застосування цього Регламенту;

f) видає настанови, рекомендації та інформацію про досвід, згідно з пп. *e* цього пункту, для подальшого визначення критеріїв і умов ухвалення рішень, що ґрунтуються на профайлінгу, відповідно до ст. 22 (2);

g) видає настанови, рекомендації та інформацію про досвід, згідно з пп. *e* цього пункту, для встановлення порушень захисту персональних даних і визначення неналежної затримки, згаданої в ст. 33 (1) і (2), та для конкретних обставин, за яких необхідно, щоб контролер або оператор повідомляли про порушення захисту персональних даних;

h) видає настанови, рекомендації та інформацію про досвід, згідно з пп. *e* цього пункту, щодо обставин, за яких порушення захисту персональних даних ймовірно створюватиме високий ризик для прав і свобод фізичних осіб, згаданих у ст. 34 (1);

i) видає настанови, рекомендації та інформацію про досвід, згідно з пп. *e* цього пункту, з метою подальшого визначення критеріїв і вимог до передавання персональних даних на підставі зобов'язальних корпоративних правил, яких дотримуються контролери, і зобов'язальних корпоративних правил, яких дотримуються оператори, а також вимог, які висуваються для забезпечення захисту персональних даних залучених суб'єктів даних, згаданих у ст. 47;

j) видає настанови, рекомендації та інформацію про досвід, згідно з пп. *e* цього пункту, для подальшого уточнення критеріїв і вимог до передавання персональних даних на підставі ст. 49 (1);

k) розробляє настанови для наглядових органів щодо застосування заходів, вказаних у ст. 58 (1), (2) і (3), та встановлення адміністративних штрафів, відповідно до ст. 83;

l) переглядає практичне застосування настанов, рекомендацій і прикладів ефективного досвіду, вказаних у пп. *e* і *f*;

m) видає настанови, рекомендації та інформацію про досвід застосування, згідно з пп. *e* цього пункту, для запровадження спільних процедур через звітування фізичними особами про порушення цього Регламенту, згідно зі ст. 54 (2);

n) заохочує розроблення кодексів поведінки та запровадження механізмів сертифікації захисту даних, штампів і знаків захисту даних, згідно зі ст. 40 і 42;

o) проводить акредитацію органів сертифікації, здійснює періодичний перегляд, відповідно до ст. 43, веде публічний

реєстр акредитованих органів, відповідно до ст. 43 (6), та акредитованих контролерів або операторів, які мають свої осідки в третіх країнах, згідно зі ст. 42 (7);

p) визначає вимоги, викладені в ст. 43 (3), для акредитації органів сертифікації, згідно зі ст. 42;

q) надає Комісії висновок щодо вимог до сертифікації, викладених у ст. 43 (8);

r) надає Комісії висновок щодо іконок, вказаних у ст. 12 (7);

s) надає Комісії висновок для оцінювання належності рівня захисту в третій країні чи міжнародній організації, в тому числі для оцінювання, чи забезпечує третя країна, територія чи один або декілька визначених секторів у межах третьої країни, чи міжнародна організація належний рівень захисту даних. З цією метою Комісія надає Раді всю необхідну документацію, в тому числі кореспонденцію з урядом третьої країни, щодо такої третьої країни, території чи визначеного сектору, чи з міжнародною організацією.

t) видає висновки щодо проектів рішень наглядових органів, відповідно до механізму послідовності, описаного в ст. 64 (1), стосовно питань, поданих відповідно до ст. 64 (2), та видає зобов'язальні рішення, відповідно до ст. 65, у тому числі для випадків, передбачених ст. 66;

u) заохочує співпрацю та ефективний двосторонній і багатосторонній обмін між наглядовими органами інформацією та досвідом;

v) сприяє спільним навчальним програмам і забезпечує можливість обмінів персоналом між наглядовими органами та, за необхідності, з наглядовими органами третіх країн або з міжнародними організаціями;

w) сприяє обміну знаннями та документацією щодо законодавства із захисту даних і досвідом з органами нагляду за захистом даних у всьому світі;

x) видає висновки щодо кодексів поведінки, розроблених на рівні Союзу, відповідно до ст. 40 (9); і

y) веде загальнодоступний електронний реєстр рішень, ухвалених наглядовими органами та судами щодо питань, які розглядалися за механізмом послідовності.

2. Якщо Комісія подає запит на консультацію Ради, вона може вказати часове обмеження, посилаючись на терміновість розгляду питання.

3. Рада передає свої висновки, настанови, рекомендації та інформацію про досвід застосування Комісії та комітету, вказаному в ст. 93, і публікує їх.

4. Рада, за необхідності, консультує відповідні сторони та забезпечує їх можливістю надавати коментарі у розумний строк. Рада, без обмеження ст. 76, оприлюднює результати процедури консультації.

Стаття 71

Звіти

1. Рада складає річний звіт про захист фізичних осіб у зв'язку з опрацюванням в Союзі та, у відповідних випадках, у третіх країнах і міжнародних організаціях. Звіт оприлюднюють та передають до Європейського Парламенту, Ради та Комісії.

2. Річний звіт містить перегляд практичного застосування настанов, рекомендацій і прикладів ефективного застосування, вказаних у пп. *i* ст. 70 (1), а також зобов'язальних рішень, вказаних у ст. 65.

Стаття 72

Процедура

1. Рада ухвалює рішення простою більшістю своїх членів, якщо інше не передбачено цим

Регламентом.

2. Рада ухвалює свої власні правила процедури більшістю в дві третини голосів своїх членів і розробляє власні технічні заходи.

Стаття 73

Голова

1. Рада обирає голову і двох заступників голови з числа своїх членів простою більшістю голосів.

2. Строк повноважень Голови і заступників Голови становить п'ять років з можливістю переобрання на повторний строк.

1. Голова має такі завдання:

Стаття 74

Завдання Голови

a) скликати засідання Ради та готувати його порядок денний;

b) повідомляти керівний наглядовий орган і залучені наглядові органи про рішення, схвалені Радою, відповідно до ст. 65;

c) забезпечувати вчасне виконання завдань Ради, зокрема, щодо механізму послідовності, описаного в ст. 63.

2. Рада розподіляє завдання між Головою та заступниками Голови в своїх правилах процедури.

Стаття 75

Секретаріат

1. Рада повинна мати секретаріат, який забезпечує Європейський інспектор із захисту даних.

2. Секретаріат виконує свої завдання винятково під керівництвом Голови Ради.

3. На персонал Європейського інспектора із захисту даних, залучений до виконання завдань, покладених на Раду згідно з цим Регламентом, поширюється механізм підзвітності, що відрізняється від механізму для персоналу, залученого до виконання завдань, покладених на Європейського інспектора із захисту даних.

4. За необхідності, Рада і Європейський інспектор із захисту даних готують і публікують Меморандум про взаєморозуміння для імплементації цієї статті, визначаючи умови своєї співпраці, який застосовують до персоналу Європейського інспектора із захисту даних, залученого до виконання завдань, покладених на Раду цим Регламентом.

5. Секретаріат надає аналітичну, адміністративну та логістичну підтримку Раді.

6. Секретаріат несе відповідальність, зокрема за:

a) повсякденну роботу Ради;

b) взаємодію між членами Ради, її Головою та Комісією;

c) взаємодію з іншими установами та громадськістю;

d) використання електронних засобів для внутрішньої та зовнішньої взаємодії;

e) переклад належної інформації;

f) підготування зустрічей Ради та виконання ухвалених на них рішень;

g) підготування, розроблення та опублікування висновків, рішень щодо врегулювання спорів між наглядовими органами та інших текстів, ухвалених Радою.

Стаття 76

Конфіденційність

1. Обговорення Ради є конфіденційними, якщо Рада вважає це необхідним, як передбачено її процедурними правилами.

2. Доступ до документів, поданих членами Ради, експертами і представниками третіх сторін, регулюється Регламентом Європейського Парламенту і Ради (ЄС) № 1049/2001*.

Розділ VIII. Засоби правового захисту, відповідальність і санкції

Стаття 77

Право на подання скарги до наглядового органу

1. Без обмеження будь-якого іншого адміністративного або судового засобу правового захисту, кожний суб'єкт даних повинен мати право на подання скарги до наглядового органу, зокрема, в державі-члені за місцем постійного проживання, місцем роботи чи місцем заявленого порушення, якщо суб'єкт даних вважає, що опрацювання його або її персональних даних суперечить положенням цього Регламенту.

2. Наглядовий орган, до якого подано скаргу, повідомляє позивача про стан і результати розгляду скарги, в тому числі про можливість судового засобу правового захисту, відповідно до ст. 78.

---

* Регламент Європейського Парламенту і Ради (ЄС) № 1049/2001 від 30 травня 2001 р. про публічний доступ до документів Європейського Парламенту, Ради і Комісії (OB L 145, 31.05.2001, с. 43).

Стаття 78

Право на дієвий судовий засіб правового захисту проти наглядового органу

1. Без обмеження будь-якого іншого адміністративного або несудового засобу правового захисту, кожна фізична або юридична особа повинна мати право на дієвий судовий засіб правового захисту від юридично зобов'язального рішення наглядового органу щодо неї.

2. Без обмеження будь-якого іншого адміністративного або несудового засобу правового захисту, будь-який суб'єкт даних повинен мати право на дієвий судовий засіб правового захисту, якщо наглядовий орган, компетентний відповідно до ст. 55 і 56, не розглядає скаргу або не інформує суб'єкта даних протягом трьох місяців про стан і результати розгляду скарги, поданої відповідно до ст. 77.

3. Провадження щодо наглядового органу здійснюють у судах держави-члена, в якій створено наглядовий орган.

4. Якщо провадження здійснюють щодо рішення наглядового органу, якому передували висновок або рішення Ради за механізмом послідовності, наглядовий орган переадресовує такий висновок або рішення до суду.

Стаття 79

Право на дієвий судовий засіб правового захисту проти контролера або оператора

1. Без обмеження будь-якого наявного адміністративного або судового засобу правового захисту, в тому числі права на подання скарги до наглядового органу, відповідно до ст. 77, кожний суб'єкт даних повинен мати право на дієвий судовий засіб правового захисту, якщо вважає, що його права за цим Регламентом порушено внаслідок опрацювання його персональних даних, що суперечить цьому Регламенту.

2. Провадження щодо контролера або оператора здійснюють у судах держави-члена, в якій має осідок контролер або оператор. Крім того, таке провадження можна здійснювати в судах держави-члена за місцем постійного проживання суб'єкта даних, за винятком випадків, коли контролер або оператор є

публічним органом держави-члена, що діє у процесі виконання своїх публічних повноважень.

Стаття 80

Представництво суб'єктів даних

1. Суб'єкт має право уповноважити неприбутковий орган, організацію чи асоціацію, засновану належним чином, відповідно до законодавства держави-члена, яка має статутні цілі в межах суспільного інтересу та активно діє в сфері захисту прав і свобод суб'єктів даних щодо захисту їхніх персональних даних, подати від його або її імені скаргу до наглядового органу, реалізовувати права, передбачені ст. 77, 78 і 79, від його або її імені, та реалізувати право на отримання відшкодування, передбачене в ст. 82, від його або її імені, як цього вимагає законодавство держави-члена.

2. Держави-члени можуть передбачити, щоб будь-який орган, організація чи асоціація, вказані в п. 1 цієї статті, мали право подати скаргу в такій державі-члені, до наглядового органу, що компетентний відповідно до ст. 77, і реалізувати права, передбачені в ст. 78 і 79, якщо вважає, що права суб'єкта даних за цим Регламентом порушено внаслідок опрацювання.

Стаття 81

Призупинення провадження

1. Якщо компетентний суд держави-члена володіє інформацією про провадження щодо того самого питання, яке стосується опрацювання тим самим контролером або оператором, яке здійснюють у суді в іншій державі-члені, він повинен звернутися до такого суду в іншій державі-члені для того, щоб підтвердити факт такого провадження.

2. Якщо провадження щодо того самого питання, яке стосується опрацювання тим самим контролером або оператором, здійснюють у суді в іншій державі-члені, будь-який компетентний суд, що не є судом, який першим розпочав провадження, може призупинити своє провадження.

3. Якщо таке провадження перебуває на розгляді в суді першої інстанції, будь-який суд, що не є судом, який першим розпочав провадження, також може, за поданням однієї зі сторін,

відмовитися від юрисдикції, якщо суд, який першим розпочав провадження, має юрисдикцію щодо дій, що розглядаються, і за його законодавством дозволено об'єднання таких проваджень.

Стаття 82

Право на відшкодування та відповідальність

1. Будь-яка особа, що зазнала матеріальної або нематеріальної шкоди внаслідок порушення цього Регламенту, має право на отримання відшкодування від контролера або оператора за заподіяну шкоду.

2. Будь-який контролер, залучений до опрацювання, несе відповідальність за шкоду, заподіяну опрацюванням, що суперечить положенням цього Регламенту. Оператор несе відповідальність за шкоду, заподіяну опрацюванням лише тоді, коли він не виконує обов'язків, передбачених цим Регламентом і спрямованих безпосередньо на оператора, або якщо він діє поза чи всупереч законним вказівкам контролера.

3. Контролер або оператор звільняються від відповідальності за п. 2, якщо доведуть, що жодним чином не несуть відповідальності за подію, що спричинила шкоду.

4. У разі залучення декількох контролерів чи операторів, або їх обох, до того самого опрацювання, та якщо вони, відповідно до п. 2 і 3, несуть відповідальність за будь-яку шкоду, спричинену опрацюванням, кожний контролер або оператор повинен нести відповідальність за заподіяння шкоди у повному обсязі з метою забезпечення дієвого відшкодування суб'єкту даних.

5. Якщо контролер або оператор, відповідно до п. 4, повністю відшкодували заподіяну шкоду, такий контролер або оператор мають право вимагати від інших контролерів або операторів, залучених до того самого опрацювання, тієї частини відшкодування, що відповідає їхній частці відповідальності за шкоду, відповідно до умов, визначених у п. 2.

6. Судове провадження щодо реалізації права на отримання відшкодування здійснюють у судах, що є компетентними, відповідно до законодавства держави-члена, як зазначено в ст. 79 (2).

Стаття 83

Загальні умови накладання адміністративних штрафів

1. Кожний наглядовий орган повинен забезпечити, щоб накладення адміністративних штрафів, відповідно до цієї ст. у зв'язку з порушеннями цього Регламенту, вказаними в п. 4, 5 і 6, у кожному окремому випадку було дієвим, пропорційним і стримувальним.

2. Адміністративні штрафи, залежно від обставин, накладають як доповнення до заходів, вказаних у пп. *a*-*h* і *j* ст. 58 (2), чи замість них. Вирішуючи, накладати адміністративний штраф чи ні і визначаючи розмір адміністративного штрафу, в кожному окремому випадку необхідно враховувати таке:

a) специфіку, ступінь тяжкості і тривалість порушення, зважаючи на специфіку, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, і розмір заподіяної їм шкоди;

b) навмисний або недбалий характер порушення;

c) будь-які заходи, вжиті контролером або оператором для зниження рівня шкоди, заподіяної суб'єктами даних;

d) ступінь відповідальності контролера або оператора, зважаючи на технічні та організаційні інструменти, які вони застосовують, відповідно до ст. 25 і 32;

e) будь-які попередні порушення з боку контролера або оператора;

f) рівень співпраці з наглядовим органом для виправлення порушення і скорочення його можливих негативних наслідків;

g) категорії персональних даних, на які вплинуло порушення;

h) спосіб, у який наглядовому органу стало відомо про порушення, зокрема, або, і якщо так, то якою мірою контролер або оператор повідомив про порушення;

i) якщо заходи, передбачені в ст. 58 (2), були раніше вжиті стосовно іншого контролера або оператора щодо такого самого порушення, – відповідність цим заходам;

j) дотримання затверджених кодексів поведінки, відповідно до ст. 40, або затверджених кодексів поведінки, відповідно до ст. 42; і

k) будь-який інший обтяжувальний або пом'якшувальний фактор, застосовний до обставин справи, такий як отримана фінансова вигода або витрати, яких вдалося уникнути, прямо чи опосередковано.

3. Якщо контролер або оператор навмисно чи через недбалість при виконанні тих самих чи пов'язаних операцій опрацювання порушує декілька положень цього Регламенту, загальна сума адміністративного штрафу не повинна перевищувати суму, визначену для найтяжчого порушення.

4. На порушення таких положень, згідно з п. 2, поширюється застосування адміністративних штрафів сумою до 10 000 000 євро, а стосовно підприємства – до 2% загального річного обігу за попередній фінансовий рік, залежно від того, яка сума вища:

a) обов'язки контролера і оператора, відповідно до ст. 8, 11, 25–39, і 42, і 43;

b) обов'язки органу з сертифікації, відповідно до ст. 42 і 43;

c) обов'язки органу з моніторингу, відповідно до ст. 41 (4);

5. На порушення таких положень, згідно з п. 2, поширюється застосування адміністративних штрафів сумою до 20 000 000 євро, а стосовно підприємства – до 4% загального річного обігу за попередній фінансовий рік, залежно від того, яка сума вища:

a) основні принципи опрацювання, в тому числі умови надання згоди, відповідно до ст. 5, 6, 7 і 9;

b) права суб'єктів даних, відповідно до ст. 12–22;

c) акти передавання персональних даних до одержувача в третій країні чи до міжнародної організації, відповідно до ст. 44–49;

d) будь-які обов'язки, відповідно до закону держави-члена, ухваленого згідно з розділом IX;

e) невідповідність постанові або тимчасовому чи остаточному обмеженню на опрацювання чи призупинення потоків даних наглядового органу, відповідно до ст. 58 (2), або ненадання доступу як порушення ст. 58 (1).

6. На невідповідність постанові наглядового органу, як зазначено в ст. 58 (2), згідно з п. 2 цієї статті, поширю-

ється застосування адміністративних штрафів сумою до 20 000 000 євро або, стосовно підприємства, – до 4% загального річного обігу за попередній фінансовий рік, залежно від того, яка сума вища.

7. Без обмеження виправних повноважень наглядових органів, відповідно до ст. 58 (2), кожна держава-член може запроваджувати правила щодо того, чи дозволено та якою мірою дозволено накладати адміністративні штрафи на публічні органи, що мають осідок у такій державі-члені.

8. Реалізація наглядовим органом своїх повноважень за цією ст. підлягає належним процесуальним гарантіям, відповідно до законодавства Союзу або держави-члена, в тому числі дієвим судовим засобам правового захисту та належному процесу.

9. Якщо правова система держави-члена не передбачає адміністративні штрафи, цю статтю можна застосовувати у такий спосіб, щоб штраф ініціював компетентний наглядовий орган і накладали компетентні національні суди, водночас забезпечуючи, щоб такі засоби правового захисту були результативними та мали дію, аналогічну до адміністративних штрафів, накладених наглядовими органами. У будь-якому разі накладені штрафи повинні бути дієвими, пропорційними і стримувальними. Такі держави-члени повідомляють Комісію про положення своїх законів, які вони ухвалюють відповідно цього розділу, до 25 травня 2018 р. та, без затримки, про будь-які подальші зміни і доповнення, що на них впливають.

Стаття 84

Санкції

1. Держави-члени запроваджують правила щодо інших санкцій, застосовних за порушення цього Регламенту, зокрема, за порушення, що не підлягають накладенню адміністративних штрафів відповідно до ст. 83, і вживають усіх заходів, необхідних для забезпечення їх реалізації. Такі санкції повинні бути дієвими, пропорційними та стримувальними.

2. Кожна держава-член повідомляє Комісію про положення свого закону, який вона ухвалює, відповідно до п. 1,

до 25 травня 2018 р. та, без затримки, про будь-які подальші зміни і доповнення, що на них впливають.

Розділ IX. Положення про спеціальні ситуації опрацювання

Стаття 85

Опрацювання і свобода вияву поглядів та свобода інформації

1. Держави-члени повинні на законодавчому рівні узгодити право на захист персональних даних, відповідно до цього Регламенту, з правом на свободу вияву поглядів і свободу інформації, в тому числі опрацювання для цілей журналістики та цілей наукової, художньої чи літературної діяльності.

2. Для опрацювання, яке здійснюють для цілей журналістики чи цілей наукової, художньої чи літературної діяльності, держави-члени повинні передбачити винятки з положень розділу II (принципи), розділу III (права суб'єкта даних), розділу IV (контролер і оператор), розділу V (передавання персональних даних до третіх країн або міжнародних організацій), розділу VI (незалежні наглядові органи), розділу VII (співпраця та послідовність) і розділу IX (особливі ситуації опрацювання даних), якщо вони необхідні для узгодження права на захист персональних даних зі свободою вияву поглядів і свободою інформації.

3. Кожна держава-член повідомляє Комісію про положення її законодавства, ухвалені нею, відповідно до п. 2, і, без затримки, про будь-який подальший закон про поправки або зміни і доповнення, що на них впливають.

Стаття 86

Опрацювання і доступ громадськості до офіційних документів

Персональні дані в офіційних документах, що зберігаються публічним органом або приватним органом для виконання завдання в суспільних інтересах, може розкрити орган або організація, відповідно до законодавства Союзу або держави-члена, яке поширюється на публічний орган або орга-

нізацію, з метою узгодження публічного доступу до офіційних документів із правом на захист персональних даних відповідно до цього Регламенту.

Стаття 87

Опрацювання національного ідентифікаційного номера

Держави-члени можуть у подальшому визначити особливі умови опрацювання національного ідентифікаційного номера чи будь-якого іншого ідентифікатора загального застосування. У такому разі національний ідентифікаційний номер або будь-який інший ідентифікатор загального застосування використовують лише за відповідних гарантій для прав і свобод суб'єкта даних, відповідно до цього Регламенту.

Стаття 88

Опрацювання в контексті зайнятості

1. Держави-члени можуть, за допомогою закону чи колективних угод, передбачати спеціальні норми для забезпечення захисту прав і свобод щодо опрацювання персональних даних працівників у контексті зайнятості, зокрема для цілей працевлаштування, виконання трудового договору, в тому числі виконання обов'язків, передбачених 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 і користування, індивідуально чи колективно, правами та перевагами, пов'язаними із зайнятістю, та для цілей припинення трудових відносин.

2. Такі норми повинні включати відповідні і спеціальні заходи захисту людської гідності суб'єкта даних, законних інтересів і фундаментальних прав, передбачати прозорість опрацювання, передавання персональних даних у межах групи підприємств або групи підприємств, що провадять спільну господарську діяльність, і системи моніторингу на робочому місці.

3. Кожна держава-член повідомляє Комісію про такі положення свого закону, який вона ухвалює, відповідно до п. 1, до 25 травня 2018 р. та, без затримки, про будь-які подальші зміни і доповнення, що на них впливають.

Стаття 89

Гарантії та відступи, що стосуються опрацювання з метою задоволення суспільних інтересів, для цілей наукового чи історичного дослідження або статистичних цілей

1. Опрацювання з метою задоволення суспільних інтересів, для цілей наукового чи історичного дослідження або статистичних цілей передбачає застосування відповідних гарантій, згідно з цим Регламентом, для прав і свобод суб'єкта даних. Такі гарантії забезпечують наявність технічних і організаційних інструментів, зокрема, для забезпечення дотримання принципу мінімізації даних. Такі заходи можуть передбачати використання псевдонімів, за можливості досягти у такий спосіб зазначених цілей. Якщо таких цілей можна досягти у ході подальшого опрацювання, що не дозволяє чи більше не дозволяє ідентифікації суб'єктів даних, зазначені цілі досягають у вказаний спосіб.

2. Якщо персональні дані опрацьовують для досягнення цілей наукового чи історичного дослідження або статистичних цілей, законодавство Союзу або держави-члена може передбачати винятки з правил, викладених у ст. 15, 16, 18 і 21, з урахуванням умов і гарантій, вказаних у п. 1 цієї статті, якщо такі правила ймовірно унеможливлять або серйозно обмежать досягнення спеціальних цілей, і такі винятки необхідні для досягнення таких цілей.

3. Якщо персональні дані опрацьовують для задоволення суспільних інтересів, законодавство Союзу або держави-члена може передбачати винятки з правил, передбачених у ст. 15, 16, 18 і 21 з урахуванням умов і гарантій, вказаних у п. 1 цієї статті, якщо такі правила ймовірно унеможливлять або серйозно обмежать досягнення спеціальних цілей, і такі винятки необхідні для досягнення таких цілей.

4. Якщо опрацювання, вказане в п. 2 і 3, слугує водночас іншій цілі, винятки застосовують лише до опрацювання для цілей, вказаних у цих пунктах.

Стаття 90

Обов'язки збереження таємниці

1. Держави-члени можуть ухвалювати спеціальні норми для визначення повноважень наглядових органів, установлених у пп. *e* і *f* ст. 58 (1), щодо контролерів або операторів, на яких поширюється, відповідно до законодавства Союзу або держав-членів або норм, встановлених національними компетентними органами, обов'язок збереження професійної таємниці чи інших подібних обов'язків збереження таємниці, якщо це необхідно і пропорційно для узгодження права на захист персональних даних з обов'язком збереження таємниці. Такі норми застосовують лише щодо персональних даних, які контролер або оператор отримав внаслідок чи під час діяльності, на яку поширюється такий обов'язок збереження таємниці.

2. Кожна держава-член повинна повідомити Комісію про норми, ухвалені відповідно до п. 1, до 25 травня 2018 р. та, без затримки, про будь-які подальші зміни та доповнення, що впливають на них.

Стаття 91

Чинні правила захисту даних церков і релігійних організацій

1. Якщо в державі-члені церкви та релігійні організації або спільноти застосовують, у день набуття чинності цим Регламентом, всеосяжні правила щодо захисту фізичних осіб у зв'язку з опрацюванням даних, такі правила можна продовжувати застосовувати, за умови їх узгодження з цим Регламентом.

2. Церкви та релігійні організації, які застосовують всеосяжні правила, згідно з п. 1 цієї статті, підлягають нагляду незалежного наглядового органу, який може бути спеціальним, за умови, що він дотримується умов, викладених у розділі VI цього Регламенту.

Розділ X. Делеговані акти та імплементаційні акти

Стаття 92

Здійснення делегування

1. Повноваження на ухвалення делегованих актів надаються Комісії з дотриманням умов, викладених у цій статті.

2. Делеговані повноваження, зазначені в ст. 12 (8) і ст. 43 (8), надаються Комісії на невизначений час, починаючи з 24 травня 2016 р.

3. Європейський Парламент або Рада можуть у будь-який час відкликати делеговані повноваження, зазначені в ст. 12 (8) і 43 (8). Рішення про відкликання припиняє делеговані повноваження, вказані в такому рішенні. Воно набуває чинності наступного дня після його публікації в Офіційному віснику Європейського Союзу або в пізнішу вказану дату. Воно не впливає на чинність будь-яких делегованих актів, що вже набули сили.

4. Ухваливши делегований акт, Комісія одразу передає його Європейському Парламенту і Раді.

5. Делегований акт, ухвалений відповідно до ст. 12 (8) і ст. 43 (8), набуває чинності тільки в тому випадку, якщо ні Європейський Парламент, ні Рада не висловили жодних заперечень протягом тримісячного періоду від дати передання зазначеного акта Європейському Парламенту і Раді, або, якщо до закінчення такого терміну і Європейський Парламент і Рада повідомили Комісію про те, що не матимуть заперечень. Такий період подовжується ще на три місяці з ініціативи Європейського Парламенту або Ради.

Стаття 93

Процедура Комітету

1. Комісії допомагає комітет. Комітет є комітетом у значенні Регламенту (ЄС) № 182/2011.

2. У разі покликання на цей пункт необхідно застосовувати ст. 5 Регламенту (ЄС) № 182/2011.

3. У разі покликання на цей пункт необхідно застосовувати ст. 8 Регламенту (ЄС) № 182/2011 у поєднанні зі ст. 5.

Розділ XI. Прикінцеві положення

Стаття 94

Скасування Директиви 95/46/ЄС

1. Директива 95/46/ЄС скасовується з 25 травня 2018 р.

2. Покликання на скасовані Директиви необхідно тлумачити як покликання на цю Директиву. Покликання на Робочу

групу із захисту осіб у зв'язку з опрацюванням персональних даних, створену ст. 29 Директиви 95/46/ЄС, необхідно тлумачити як покликання на Європейську Раду із захисту даних, створену цим Регламентом.

Стаття 95

Взаємозв'язок із Директивою 2002/58/ЄС

Регламент не покладає додаткових обов'язків на фізичних або юридичних осіб у зв'язку з опрацюванням у сфері постачання послуг електронного зв'язку, що є публічно доступними, в комунікаційних мережах загального доступу в Союзі щодо питань, за якими вони підлягають виконанню конкретних обов'язків з тією самою метою, встановленою в Директиві 2002/58/ЄС.

Стаття 96

Взаємозв'язок із попередньо укладеними угодами

Міжнародні угоди, що передбачають передавання персональних даних до третіх країн або міжнародних організацій і були укладені державами-членами до 24 травня 2016 р. та відповідають праву Союзу як застосовні до такої дати, залишаються чинними до внесення змін і доповнень, заміни чи скасування.

Стаття 97

Звіти Комісії

1. До 25 травня 2020 р. та кожні чотири роки після цієї дати Комісія подає звіт про оцінювання та перевірку виконання цього Регламенту до Європейського Парламенту та Ради. Звіти необхідно оприлюднити.

2. У контексті оцінювань і перевірок, вказаних у п. 1, Комісія вивчає, зокрема, застосування та функціонування:

a) Розділу V щодо передавання персональних даних до третіх країн або міжнародних організацій з особливим урахуванням рішень, ухвалених відповідно до ст. 45 (3) цього Регламенту та рішень, ухвалених на підставі ст. 25 (6) Директиви 95/46/ЄС;

b) Розділу VII про співпрацю і послідовність.

3. Для цілі п. 1 Комісія може надати запит на отримання інформації від держав-членів і наглядових органів.

4. Проводячи оцінювання та перевірки, вказані в п. 1 та 2, Комісія враховує позиції та висновки Європейського Парламенту, Ради та інших відповідних органів і джерел.

5. Комісія, якщо необхідно, подає відповідні пропозиції для внесення змін і доповнень до цього Регламенту, зокрема, враховуючи розвиток інформаційних технологій і досягнення прогресу інформаційного суспільства.

Стаття 98

Перевірка застосування інших нормативно-правових актів Союзу щодо захисту даних

Комісія, у належних випадках, подає законодавчі пропозиції з метою внесення змін до інших нормативно-правових актів Союзу щодо захисту персональних даних, для того, щоб забезпечити єдиний і послідовний захист фізичних осіб у зв'язку з опрацюванням. Вони, зокрема, стосуються норм щодо захисту фізичних осіб у зв'язку з опрацюванням установами, органами, службами та агентствами Союзу та щодо вільного переміщення таких даних.

Стаття 99

Набуття чинності та застосування

1. Цей Регламент набуває чинності на 20-й день після його публікації в Офіційному віснику Європейського Союзу.

2. Він застосовується з 25 травня 2018 р.

Цей Регламент обов'язковий у повному обсязі та підлягає прямому застосуванню в усіх державах-членах.

Учинено в Брюсселі 27 квітня 2016 р.
За Європейський Парламент
Президент
M. SCHULZ
За Раду
Президент
J.A. HENNIS-PLASSCHAERT