I

(Законодавчі акти)

РЕГЛАМЕНТИ

РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/679

від 27 квітня 2016 року

про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та 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 статтю 16,

Беручи до уваги пропозицію Європейської Комісії,

Після передавання проекту законодавчого акта національним парламентам,

Беручи до уваги висновок Європейського економічно-соціального комітету ([1]),

Беручи до уваги висновок Комітету регіонів ([2]),

Діючи згідно зі звичайною законодавчою процедурою ([3]),

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, економічного 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 ([4]) спрямовано на гармонізацію захисту фундаментальних прав і свобод фізичних осіб під час опрацювання персональних даних та забезпечення вільного руху персональних даних між державами-членами.

([1]) ОВ С 229, 31.07.2012, с. 90.
([2]) ОВ С 391, 18.12.2012, с. 127.
([3]) Позиція Європейського Парламенту від 12 березня 2014 року (ще не опубліковано в Офіційному віснику) і позиція Ради в першому читанні від 8 квітня 2016 року (ще не опубліковано в Офіційному віснику). Позиція Європейського Парламенту від 14 квітня 2016 року.
([4]) Директива Європейського Парламенту і Ради 95/46/ЄС від 24 жовтня 1995 року про захист осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (ОВ L 281, 23.11.1995, с. 31).

I

(Законодавчі акти)

РЕГЛАМЕНТИ

РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/679

від 27 квітня 2016 року

про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та 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 статтю 16,

Беручи до уваги пропозицію Європейської Комісії,

Після передавання проекту законодавчого акта національним парламентам,

Беручи до уваги висновок Європейського економічно-соціального комітету ([1]),

Беручи до уваги висновок Комітету регіонів ([2]),

Діючи згідно зі звичайною законодавчою процедурою ([3]),

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, економічного 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 ([4]) спрямовано на гармонізацію захисту фундаментальних прав і свобод фізичних осіб під час опрацювання персональних даних та 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 повинне розглядатися в зв'язку з

([1]) ОВ C 229, 31.07.2012, с. 90.
([2]) ОВ C 391, 18.12.2012, с. 127.
([3]) Позиція Європейського Парламенту від 12 березня 2014 року (ще не опубліковано в Офіційному віснику) і позиція Ради в першому читанні від 8 квітня 2016 року (ще не опубліковано в Офіційному віснику). Позиція Європейського Парламенту від 14 квітня 2016 року.
([4]) Директива Європейського Парламенту і Ради 95/46/ЄС від 24 жовтня 1995 року 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 в 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 та 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 дозволяють 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 наявності міцних та більш узгоджених засад щодо захисту даних у Союзі, із запровадженням належного механізму виконання, беручи до уваги важливість формування довіри, що дозволить розвиток цифрової економіки на рівні внутрішнього ринку. Фізичні особи повинні мати контроль щодо власних персональних даних. Необхідно зміцнити правову та практичну визначеність для фізичних осіб, суб'єктів господарювання і органів публічної влади.

(8) Якщо цим Регламентом передбачено уточнення або обмеження його норм законодавством держав-членів, у такому разі останні можуть, мірою необхідності узгодження і забезпечення розуміння положень національного законодавства особами, на які вони поширюються, інкорпорувати елементи цього Регламенту у 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 рівні 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 потоку персональних даних всередині Союзу. Відповідно, такі відмінності можуть перешкоджати веденню 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 в ході імплементації та застосування Директиви 95/46/ЄС.

(10) Для забезпечення сталого та високого рівня захисту фізичних осіб і 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 для відповідності встановленим законом зобов'язанням, для виконання завдання суспільних інтересів або для здійснення офіційних повноважень, покладених на контролера, державам-членам необхідно дозволити мати або вводити положення національного законодавства для більш детального уточнення 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 більш уточнених положень. Цей Регламент також надає простір для маневру для держав-членів 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 і приймають рішення щодо опрацювання персональних даних, а також надання рівнозначних повноважень з моніторингу і забезпечення дотримання норм щодо захисту персональних даних та 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 та 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 у всіх 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 їхні наглядові органи закликають враховувати особливі потреби мікропідприємств, малих і середніх підприємств у ході застосування цього Регламенту. Поняття мікропідприємтв, малих і середніх підприємств повинно відповідати означенню, яке містять положення статті 2 додатку до Рекомендації Комісії 2003/361/ЄС ([1]).

(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 та, 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 або призначення для

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

внесення до картотеки. На файли або групи файлів, а також їхні титульні сторінки, які не структуровано за спеціальними критеріями, дія цього Регламенту не поширюється.

(16) Цей Регламент не застосовують до питань захисту фундаментальних прав і свобод або вільного потоку персональних даних, пов'язаних з діяльністю поза межами законодавства Союзу, наприклад, 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 ([1]) 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 та 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 або комерційною діяльністю. Особисту або побутову діяльність може становити ведення кореспонденції та зберігання адрес, або 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 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 ([2]). 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, в частині, що стосується сфери застосування законодавства Союзу, поширюється дія 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 вводити 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

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

([2]) Директива Європейського Парламенту і Ради (ЄС) 2016/680 від 27 квітня 2016 року 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).

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 та 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 є доцільним наприклад у контексті боротьби проти відмивання грошей або діяльності лабораторій судових експертиз.

(20) Оскільки дія цього Регламенту поширюється, між іншим, на діяльність судів і 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 їхньої 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 рамках 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 ([1]), зокрема норм статей 12–15 зазначеної Директиви про відповідальність надавачів посередницьких послуг. Зазначену Директиву спрямовано на сприяння належному функціонуванню внутрішнього ринку шляхом забезпечення вільного руху надання послуг інформаційного суспільства між державами-членами.

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

(23) Для того, щоб забезпечити, що фізичних осіб не позбавлено захисту, на який вони мають право за цим Регламентом, на опрацювання персональних даних суб'єктів даних, які перебувають в 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 в 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 рамках 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.

([1]) Директива Європейського Парламенту і Ради 2000/31/ЄС від 8 червня 2000 року 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).

(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 здійснюють для 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 прийняття 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 псевдоніму, що 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 взяти до уваги 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. Таким чином 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 вводити норми щодо опрацювання персональних даних померлих осіб.

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

(29) Для створення стимулів використання псевдоніму під час опрацювання персональних даних, заходи щодо використання псевдоніму повинні, дозволяючи при цьому загальний аналіз, уможливлювати їхнє 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 до певного суб'єкта даних зберігають окремо. Контролер, що здійснює опрацювання персональних даних, повинен зазначити уповноважених осіб серед 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 встановленого 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 проведення 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 здійснювати опрацювання персональних даних відповідно до застосовних норм щодо захисту даних та цілей опрацювання.

(32) Згоду необхідно надавати шляхом чіткого ствердження, що становить вільно надане, конкретне, проінформоване та однозначне свідчення погодження суб'єкта даних на опрацювання його або її персональних даних, зокрема, у формі письмової заяви, в тому числі електронними засобами, або у формі усної заяви. Це може включати заповнення клітинки позначкою під час відвідування веб-сайту в мережі Інтернет, обрання технічних налаштувань для послуг інформаційного суспільства або іншу заяву чи поведінку, що чітко вказують на погодження суб'єктом даних із запропонованим опрацюванням персональних даних. Мовчання, автоматичне заповнення клітинок позначками або бездіяльність, відповідно, не становлять надання згоди. Згода повинна поширюватися на всі види опрацювання даних, що здійснюють для однакової цілі або цілей. У разі, 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 та не мати надмірно негативних наслідків для використання послуги, для якої його надають.

(33) Часто на момент збирання даних неможливо повністю визначити мету опрацювання персональних даних для цілей наукового дослідження. Тому, суб'єкти даних повинні мати дозвіл на надання згоди на деякі сфери наукових досліджень, якщо в них дотримано визнаних етичних норм для наукового дослідження. Суб'єкти даних повинні мати можливість надавати свою згоду лише на окремі сфери дослідження або частини дослідницьких проектів в обсязі, виправданому поставленою метою.

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

(35) Персональні дані стосовно стану здоров'я повинні містити всі дані, що пов'язані зі станом здоров'я суб'єкта даних та розкривають 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 ([1]), 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

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

надходження, наприклад, від лікаря або 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 та засобів опрацювання на основі стабільних домовленостей. Цей критерій не повинен залежати від того, чи здійснюють опрацювання персональних даних у такому місці. Наявність та використання технічних засобів та технологій опрацювання персональних даних або опрацювання даних не становлять як такі головний осідок та, відповідно, не є вирішальними критеріями для головного осідку. Головним осідком оператора повинно бути місце розташування його центральної адміністрації в Союзі або, якщо немає його центральної адміністрації в Союзі, місце, де виконують основні види опрацювання даних в 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 здійснює група підприємств, головний осідок підприємства, що здійснює контроль, необхідно вважати головним осідком групи підприємств, за винятком, якщо цілі та засоби опрацювання визначено іншим підприємством.

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

(38) Діти потребують особливого захисту в питанні персональних даних, оскільки вони можуть бути менш обізнаними про відповідні ризики, наслідки та гарантії, а також про свої права щодо опрацювання персональних даних. Такий особливий захист повинен, зокрема, застосовуватися до використання персональних даних дітей для цілей маркетингу або створення профілів особистості чи користувача та збирання персональних даних щодо дітей під час користування послугами, що 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 та 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 та законними, а також означеними на момент збирання персональних даних. Персональні дані повинні бути достатніми, відповідними та обмежуватися тим, що є необхідним для досягнення цілей, для яких їх опрацьовують. Це вимагає, зокрема, забезпечення того, що період, протягом якого зберігаються персональні дані, скорочений до абсолютного мінімуму. Персональні дані необхідно опрацьовувати, лише якщо мети опрацювання не можна досягнути розумним чином іншими засобами. Щоб забезпечити, що персональні дані не зберігаються довше, ніж це необхідно, контролер повинен установити часові рамки для стирання або періодичного перегляду. Необхідно вживати всіх відповідних заходів для забезпечення виправлення або видалення 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) Для того, щоб опрацювання було законним, персональні дані необхідно опрацьовувати на підставі згоди відповідного суб'єкта даних або на іншій законній підставі, встановленій законом, або у цьому Регламенті, або в іншому нормативно-правовому акті Союзу або держави-члена, як вказано 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 до укладення договору.

(41) Якщо цей Регламент містить покликання на законодавчу базу або законодавчий інструмент, ухвалення парламентом законодавчого акту, з дотриманням вимог, що відповідають конституційному порядку відповідної держави-члена, є необов'язковим. Проте така законодавча база або такий законодавчий інструмент повинні бути чіткими та точними, а їхнє 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 ([1]) заяву про надання згоди, попередньо сформульовану контролером, необхідно надавати в зрозумілій та доступній формі з використанням чітких і простих формулювань, а також вона не повинна містити неправомірні умови. Для того, щоб згода вважалася поінформованою, суб'єкт даних повинен бути обізнаним принаймні про особу контролера та цілі опрацювання, для яких призначено використання персональних даних. Згоду не можна вважати такою, що було добровільно надано, якщо суб'єкт даних не здійснює справжнього чи добровільного вибору, або неспроможний відмовити в наданні згоди або її відкликанні, не заподіюючи при цьому шкоди.

(43) Щоб забезпечити, що згоду було надано добровільно, 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 відсутності окремого дозволу на здійснення різних операцій опрацювання персональних даних, незважаючи на її відповідність окремому випадку, або, якщо виконання договору, в тому числі, надання

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

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 здійснення офіційних повноважень, його необхідно проводити на підставі нормативно-правового акту Союзу чи держави-члена. Цей Регламент не вимагає ухвалення спеціального нормативно-правового акту для кожного окремого опрацювання. Нормативно-правового акту як основи для здійснення декількох операцій з опрацювання, що ґрунтуються на виконанні встановленого законом зобов'язання контролера, або, за умов 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 зазначати 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 можна 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, що 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 є в суспільних інтересах, у тому числі для цілей здоров'я таких 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, що є важливим 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 інтересах суб'єкта даних, наприклад, якщо опрацювання є необхідним для гуманітарних цілей, у тому числі моніторингу епідемій та їхнього розповсюдження чи у випадку 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, наприклад, якщо є 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 на подальше опрацювання. З огляду на те, що саме законодавець повинен передбачити законом 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, що

є необхідним виняткова для цілей запобігання шахрайству також становить законний інтерес відповідного контролера даних. Опрацювання персональних даних для цілей прямого маркетингу можна вважати опрацюванням, що здійснюють 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 щодо 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 та конфіденційність збережених або переданих персональних даних, і безпеки пов'язаних послуг, які пропонують через такі мережі чи системи або надають за їхньою 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 розподіл 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 є сумісним із первинними цілями збирання персональних даних. У такому разі немає необхідності в будь-якій законодавчій базі, окремій від такої, якою вже дозволено збирання персональних даних. Якщо опрацювання персональних даних є необхідним для виконання завдання в публічних інтересах або здійснення офіційних повноважень, покладених на контролера, законодавство Союзу або держави-члена може визначити та уточнити завдання і цілі, для виконання яких необхідно вважати сумісним та законним подальше опрацювання. Подальше опрацювання для архівних цілей у публічних інтересах, цілей наукового або історичного дослідження, статистичних цілей необхідно вважати сумісними 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 цілі подальшого опрацювання, для якого відбувається первинне 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; та 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 отримувати 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 їхнього 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 терміну «расова приналежність» в 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 дозволяють однозначну ідентифікацію або аутентифікацію фізичної особи. Такі персональні дані не можна опрацьовувати, за винятком, якщо це дозволено в спеціальних випадках, визначених у цьому Регламенті, беручи до уваги, що законодавство держави-члени може встановлювати 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 від 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 відступ 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 щодо врегулювання претензій на пільги та послуги в 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 рамках адміністративної чи позасудової процедури.

(53) Опрацювання спеціальних категорій персональних даних, що потребують вищого ступеня захисту, необхідно здійснювати для цілей, пов'язаних з охороною здоров'я, лише якщо необхідно досягнути таких цілей в інтересах фізичних осіб та суспільства в цілому, 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 цілі 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 цілі суспільного інтересу, а також для навчання, яке проводять в інтересах суспільства в сфері охорони суспільного здоров'я. Тому, цей Регламент повинен передбачати гармонізовані умови для опрацювання спеціальних категорій персональних даних стосовно стану здоров'я, з урахуванням особливих потреб, зокрема, якщо такі дані опрацьовують особи, на яких покладено встановлене законом 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 вводити подальші 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 потоку персональних даних в межах Союзу тоді, коли такі умови застосовують до транскордонного опрацювання таких даних.

(54) Опрацювання спеціальних категорій персональних даних може бути необхідним в цілях суспільних інтересів у галузях 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 ([1]), 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 на підставі суспільного інтересу.

(56) У ході виборчого процесу, функціонування демократичної системи в державі-члені вимагає збирання політичними партіями персональних даних про політичні переконання населення, дозвіл на опрацювання таких даних можна надавати для цілей 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 винятково для цілей дотримання будь-якого положення цього Регламенту. Проте контролер не повинен відмовлятися від додаткової інформації, яку надає суб'єкт даних для підтримки реалізації своїх прав. Ідентифікація повинна включати цифрову ідентифікацію суб'єкта даних, наприклад за допомогою механізму аутентифікації, такого

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

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, з використанням чітких і простих формулювань, 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, є доцільним у ситуаціях, коли збільшення кількості агентів і технологічна складність практичної діяльності перешкоджають обізнаності та розумінню суб'єкта 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 їхнього виправлення та стирання, а також реалізацію права на заперечення. Контролер повинен також надати засоби для уможливлення подачі 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 проінформовано про наявність операції 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 проінформувати суб'єкта даних про наявність профайлінгу та наслідки такого профайлінгу. У разі отримання персональних даних від суб'єкта даних, його або її також необхідно проінформувати 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 навести, у видимий, доступний для розуміння та чіткий спосіб, змістовний огляд запланованого опрацювання. У разі представлення іконок у електронному форматі, вони повинні легко зчитуватися машиною.

(61) Інформацію щодо опрацювання персональних даних про суб'єкта даних необхідно надавати йому або їй в 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 розкриті ще одному одержувачу, суб'єкта даних необхідно проінформувати 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 накладати обов'язок щодо надання інформації, якщо суб'єкт даних уже володіє інформацією, якщо реєстрація або розкриття персональних даних чітко встановлено 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 досягнення цілей у суспільних інтересах, цілей наукового чи історичного дослідження, статистичних

цілей. У зв’язку з такими обставинами, 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 даних, що стосуються їхнього здоров’я, наприклад даних у їхніх медичних записах, що містять інформацію, таку 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 і отримувати інформацію, зокрема про цілі, для яких опрацьовують персональні дані; за можливості, період, протягом якого опрацьовують персональні дані; одержувачів персональних даних; логіку, що обумовлює будь-яке автоматизоване опрацювання персональних даних, і принаймні, що базується на профайлінгу; наслідки такого опрацювання. За можливості, контролер повинен бути спроможним надавати віддалений доступ до системи безпеки, яка б забезпечила суб’єкту даних прямий доступ до своїх персональних даних. Таке право не повинно негативно впливати на права чи свободи інших осіб, у тому числі комерційні таємниці чи інтелектуальну власність та, зокрема, авторське право в галузі захисту програмного забезпечення. Проте наслідком таких обговорень не повинна бути відмова надати усю інформацію суб’єкту даних. Якщо контролер опрацьовує великі обсяги інформації про суб’єкта даних, він повинен мати можливість надіслати запит про те, щоб до моменту надсилання інформації суб’єкт даних вказав інформацію або види опрацювання даних, яких стосується запит.

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

(65) Суб’єкт даних повинен мати право на виправлення своїх персональних даних і «право бути забутим», якщо утримання таких даних порушує цей Регламент або законодавство Союзу чи держави-члени, яке поширюється на контролера. Зокрема, суб’єкт даних повинен мати право на видалення своїх персональних даних та припинення їхнього опрацювання, якщо персональні дані більше не є потрібними щодо цілей, для яких їх збирають або іншим чином опрацьовують, якщо суб’єкт даних відкликав свою згоду або заперечує проти опрацювання йог 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 видалити такі персональні дані, особливо з мережі Інтернет. Суб’єкт даних повинен мати можливість реалізовувати таке право, незважаючи на той факт, що він більше не є дитиною. Проте подальше утримання персональних даних повинно бути законним, за необхідності, для реалізації права на свободу вияву поглядів та свободу інформації, дотримання встановленого законом зобов’язання, виконання завдання в суспільних інтересах чи офіційних повноважень, покладених на контролера, на підставі суспільного інтересу в сфері охорони суспільного здоров’я, для досягнення цілей у суспільних інтересах, цілей наукового чи історичного дослідження, статистичних цілей, або для формування, здійснення або захисту законного права вимоги.

(66) Для посилення права бути забутим в електронному середовищі необхідно також розширити право на стирання таким чином, щоб контролер, який оприлюднив персональні дані, був зобов’язаний проінформувати контролерів, які опрацьовують такі персональні дані, стерти будь-які посилання на такі персональні, або їх копії чи відтворення. Тим самим, контролер повинен вживати відповідних заходів, враховуючи наявні технології та інструменти, доступні для контролера, в тому числі технічні інструменти, для інформування контролерів, які опрацьовують персональні дані на запит суб’єкта даних.

(67) Методи для обмеження опрацювання персональних даних можуть включати, між іншим, тимчасове перенесення обраних даних до іншої системи опрацювання, що робить їх недоступними для користувачів, або тимчасове видалення опублікованих даних зі сторінки в мережі Інтернет. В автоматизованих картотеках обмеження опрацювання необхідно, по суті, забезпечувати технічними інструментами у такий спосіб, що унеможливлює подальші операції опрацювання і зміни персональних даних. Необхідно чітко вказувати в системі те, що опрацювання персональних даних є обмеженим.

(68) Для посилення контролю за своїми власними даними, якщо персональні дані 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, що уможливлюють 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, іншої ніж згода чи договір. За своєю специфікою таке право не потрібно реалізовувати проти контролерів, які здійснюють опрацювання персональних даних під час виконання своїх службових обов'язків. Тому, 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 випадку 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 видалення персональних даних і обмеження такого права, як встановлено в цьому Регламенті, та не повинно, зокрема, передбачати видалення персональних даних про суб'єкт даних, які були надані ним або нею для виконання договору мірою та протягом періоду необхідності персональних даних для виконання договору. За умов технічної доцільності, суб'єкт даних повинен мати право на те, щоб персональні дані було передано безпосередньо від одного контролера до наступного.

(69) Якщо персональні дані можна опрацьовувати на законних підставах, оскільки опрацювання є необхідним для виконання завдання в суспільних інтересах чи здійснення офіційних повноважень, покладених на контролера, або на підставах законних інтересів контролера чи третьої сторони, у такому разі суб'єкт даних повинен, тим не менше, мати право на заперечення проти опрацювання будь-яких персональних даних, що стосуються його або її конкретної ситуації. Відповідальністю контролера є доведення, що його вагомий 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 та на безоплатній основі. Таке право необхідно однозначно довести до відома суб'єкта даних і представити чітко та окремо від будь-якої іншої інформації.

(71) Суб'єкт даних повинен мати право не дотримуватися виконання рішення, що може передбачати вжиття заходу з оцінювання його або її персональних аспектів, винятково на підставі автоматизованого опрацювання, та яке породжує правові наслідки для нього чи неї або подібним чином істотно впливає на нього чи неї, а саме, автоматичну відмову в онлайн-заявці на кредит або практику наймання працівників за допомогою Інтернет-ресурсів без будь-якого втручання людини. Таке опрацювання включає «профайлінг»,

що складається з будь-якої форми автоматизованого опрацювання персональних даних із оцінюванням персональних аспектів, що стосуються фізичної особи, зокрема для аналізу або передбачення аспектів, що стосуються продуктивності суб'єкта даних на роботі, економічної ситуації, здоров'я, особистих переваг або інтересів, надійності або поведінки, місцезнаходження або пересування, якщо воно породжує правові наслідки, що стосуються його чи її, чи подібним чином істотно впливає на нього чи неї. Проте дозвіл на вироблення й ухвалення рішень на підставі такого опрацювання, в тому числі профайлінгу, необхідно надавати в разі, якщо це чітко передбачено законодавством Союзу чи держави-члена, яке поширюється на контролера, у тому числі для цілей моніторингу, запобігання шахрайству та ухиленню від сплати податків, що здійснюють відповідно до регламентів, стандартів і рекомендацій установ Союзу чи національних органів з нагляду і для гарантування безпеки і надійності послуги, яку постачає контролер, або необхідних для укладення чи виконання договору між суб'єктом даних і контролером, або якщо суб'єкт даних надав свою чітку згоду. У будь-якому разі таке опрацювання необхідно здійснювати згідно з відповідними гарантіями, що повинні включати 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.

Для того, щоб забезпечити правомірне та прозоре опрацювання, 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, наявні для інтересів та прав суб'єкта даних, і запобігає, між іншим, 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 автоматизовані вироблення й ухвалення рішень та профайлінг на підставі спеціальних категорій персональних даних необхідно надавати лише за спеціальних умов.

(72) Профайлінг регулюють норми цього Регламенту щодо опрацювання персональних даних, такі 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 та прав на інформацію, доступ до персональних даних, їх виправлення або стирання, 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 накладати законодавством Союзу або держави-члена, наскільки це необхідно та пропорційно в демократичному суспільстві для гарантування громадської безпеки, в тому числі захисту життя людини, особливо у відповідь на стихійні лиха і антропогенні катастрофи, запобігання, розслідування і переслідування осіб за скоєння кримінальних злочинів або виконання кримінальних покарань, у тому числі захист від загроз громадській безпеці та запобігання їм, або за порушення етичних норм для регульованих професій, про інші важливі цілі загального суспільного інтересу Союзу або держави-члена, зокрема важливий економічний або фінансовий інтерес Союзу або держави-члена, ведення публічних реєстрів на підставі загального суспільного інтересу, подальше опрацювання архівних персональних даних для надання конкретної інформації, що стосується політичної поведінки під колишніми тоталітарними державними режимами або захисту суб'єктів даних або прав і свобод інших, у тому числі соціального захисту, цілей охорони здоров'я населення або гуманітарних цілей. Зазначені обмеження повинні

відповідати вимогам, установленим 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 та 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, що 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 та свобод або можливості здійснювати контроль 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 стосовно стану здоров'я або дані щодо сексуального життя або судимостей та кримінальних злочинів або пов'язаних заходів безпеки; коли оцінюють персональні аспекти, особливо із аналізом або передбаченням аспектів, що стосуються продуктивності на роботі, 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 та впливає на велику кількість суб'єктів даних.

(76) Потрібно визначати ймовірність та тяжкість ризику для прав і свобод суб'єкта даних, спираючись на специфіку, масштаб, контекст та 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 та доведення відповідності контролером або оператором, особливо в тому, що стосується 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, за допомогою узгоджених кодексів поведінки, затвердженими сертифікатами, настановами, наданими Радою, або вказівками, наданими співробітником з питань захисту даних. Рада може також видавати настанови щодо операцій опрацювання, які розглядають 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 такого ризику.

(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. Для того, 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 та захисту даних за замовчуванням. Такі заходи можуть передбачати, між іншим, скорочення опрацювання персональних даних, якомога швидше використання псевдонімів до персональних даних, прозорість щодо функцій та опрацювання персональних даних, уможливлення суб'єкта даних відстежувати опрацювання даних, уможливлення контролера створювати та

вдосконалювати характеристики безпеки. Під час створення, розроблення, відбору та використання застосунків, сервісів та продуктів, що засновано на опрацюванні персональних даних, або 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, з належним дотриманням сучасного рівня розвитку, переконуватися, що контролери і оператори здатні виконувати свої зобов'язання щодо захисту даних. Принципи захисту даних за призначенням та захисту даних за замовчуванням необхідно також брати до уваги в контексті публічних тендерів.

(79) Захист прав і свобод суб'єктів даних, а також обов'язки та відповідальність контролерів і операторів, також у зв'язку з моніторингом наглядових органів та за допомогою їхніх засобів, вимагає 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 має осідку в Союзі, опрацьовує персональні дані суб'єктів даних, які перебувають в Союзі, опрацювання даних яких 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, контролер і оператор повинні призначити представника, за винятком ситуацій, коли опрацювання призначено для окремого випадку, включає опрацювання, у великих масштабах, спеціальних категорій персональних даних або опрацювання персональних даних щодо судимостей та кримінальних злочинів, та 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, та до нього може звертатися будь-який наглядовий орган. Представника необхідно чітко призначати на підставі письмового доручення контролера або оператора діяти від його імені у контексті його зобов'язань згідно з цим Регламентом. Призначення такого представника не впливає на обов'язки або відповідальність контролера або оператора згідно з цим Регламентом. Такий 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 буде здійснювати оператор від імені контролера, який доручив оператору опрацювання даних, контролер повинен використовувати послуги лише таких операторів, які надають достатніх 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 встановлює 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 використання індивідуального договору або стандартних положень договору, ухвалених відповідно до механізму послідовності або безпосередньо Комісією або наглядовим органом, а потім — Комісією. Після завершення опрацювання від імені контролера, оператор повинен, на розсуд контролера, повернути

або видалити персональні дані, за винятком відсутності 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, здійснені в межах їхніх обов'язків. Всі контролери і оператори повинні бути зобов'язані співпрацювати з наглядовим органом і надавати йому такі записи на запит для сприяння моніторингу таких операцій опрацювання.

(83) Для гарантування безпеки та запобігання опрацюванню, що порушує цей Регламент, контролер або оператор повинні оцінювати ризики, властиві опрацюванню, та вживати заходів для зниження таких ризиків, наприклад, шифрування. Такі заходи повинні гарантувати належний рівень безпеки, в тому числі конфіденційність, у тому числі, сучасний рівень розвитку та витрати на їхню реалізацію відносно ризиків і специфіки персональних даних, що підлягають захисту. Під час оцінювання ризику для захисту даних, необхідно розглянути ризики, спричинені опрацюванням персональних даних, таким як випадкове чи незаконне знищення, втрата, зміна, несанкціоноване розкриття або доступ до персональних даних, які передають, зберігають або іншим чином опрацьовують, що, зокрема, можуть призвести до фізичної, матеріальної та нематеріальної шкоди.

(84) Для посилення ступеня відповідності цьому Регламенту в ситуаціях, коли операції опрацювання ймовірно спричиняють 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. Необхідно враховувати результати оцінювання під час визначення належних заходів, яких необхідно вжити для підтвердження того, що опрацювання персональних даних відповідає цьому Регламенту. Якщо оцінка впливу на захист даних вказує на те, що операції опрацювання містять високий ризик, який контролер не може знизити належними засобами, зважаючи на наявну технологію та витрати на їхню реалізацію, в такому разі до початку опрацювання необхідно провести консультацію для наглядового органу.

(85) Порушення захисту персональних даних може, якщо не його не розглянути своєчасно та належним чином, призвести до нанесення фізичним особам фізичної, матеріальної та нематеріальної шкоди, такої як втрата контролю над їхніми персональними даними або обмеження їхніх прав, дискримінація, крадіжка персональних даних або шахрайство, фінансові втрати, несанкціоноване скасування використання псевдонімів, шкода репутації, втрата конфіденційності персональних даних, захищених як особисту таємницю, або будь-яка інша істотна економічна або соціальна шкода відповідній фізичній особі. Таким чином, як тільки контролеру стає відомо про порушення захисту персональних даних, він повинен повідомити наглядовий орган про порушення захисту персональних даних без неналежної затримки та, за можливості, не пізніше ніж за 72 години після того, як йому стало про це відомо, за винятком якщо контролер може довести, згідно з принципом підзвітності, що порушення захисту персональних даних малоймовірно створить ризик для прав і свобод фізичних осіб. Якщо неможливо здійснити таке повідомлення протягом 72 годин, у такому разі разом із повідомленням необхідно надати відомості про причини затримки; інформацію можна надати поетапно без неналежної подальшої затримки.

(86) Контролер повинен повідомити суб'єкту даних про порушення захисту персональних даних, без неналежної затримки, якщо таке порушення захисту персональних даних ймовірно створить високий ризик для прав і свобод фізичної особи для того, щоб дозволити їй вжити необхідних запобіжних заходів. У повідомленні необхідно описати специфіку порушення захисту персональних даних, а також надати рекомендації для зазначеної фізичної особи з метою зменшення потенційних негативних наслідків. Необхідно надавати такі повідомлення суб'єктам даних якомога швидше та в тісній

співпраці з наглядовим органом, дотримуючись настанов, наданих ним або іншими відповідними органами, такими як правоохоронні органи. Наприклад, потреба знизити безпосередній ризик нанесення шкоди потребує 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 було реалізовано всі належні заходи технологічного захисту та організаційні заходи для того, щоб негайно встановити, чи відбулося порушення захисту персональних даних, а також повідомити наглядовий орган і суб'єкта даних належним чином. Необхідно встановити факт відсутності затримки в наданні повідомлення із врахуванням, зокрема, специфіки і тяжкості порушення захисту персональних даних, його наслідки та негативний вплив для суб'єкта даних. Таке надання повідомлення може спричинити втручання наглядового органу відповідно до його завдань та повноважень, встановлених у цьому Регламенті.

(88) Під час встановлення детальних правил щодо формату і процедур, застосовних до надання повідомлення про порушення захисту персональних даних, необхідно належним чином розглянути наслідки такого порушення, в тому числі, чи перебували персональні дані під захистом відповідних заходів технічного захисту, що у дієвий спосіб обмежують ймовірність крадіжки персональних даних або інші форми неправомірного використання. Більш 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. Незважаючи на те, що цей обов'язок породжує адміністративний та фінансовий тягарі, він необов'язково сприяв покращенню у сфері захисту персональних даних. Тому, такі 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 створять високий ризик для прав і свобод фізичних осіб в силу їхньої специфіки, масштабу, контексту та цілей. Такими типами операцій опрацювання можуть бути операції, які, зокрема, передбачають використання нових технологій або є новими і такими, щодо яких контролер раніше не проводив жодного оцінювання впливу на захист даних, або такими, що стають необхідними в аспекті 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 конкретну ймовірність і ступінь тяжкості високого ризику, враховуючи специфіку, обсяг, контекст і цілі опрацювання та джерела ризику. У такій оцінці необхідно вказати, зокрема, заходи, гарантії та механізми, передбачені для зниження такого ризику, які забезпечують захист персональних даних і підтверджують відповідність цьому Регламенту.

(91) Це, зокрема, необхідно застосовувати до широкомасштабних операцій опрацювання, спрямованих на опрацювання значних обсягів персональних даних на регіональному, національному чи наднаціональному рівні, які можуть вплинути на велику кількість суб'єктів даних і ймовірно створити високий ризик, наприклад враховуючи їхню чутливість, у ході якого широкомасштабно використовують нову технологію відповідно до досягнутого стану технологічних знань, а також до 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. Оцінювання впливу на захист даних також необхідно проводити, 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 або пов'язані заходи безпеки. Оцінювання впливу на захист даних є однаково необхідним для всебічного моніторингу загальнодоступних територій, особливо під час застосування 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 реалізовувати право або користуватися послугою чи договором, або тому, що їх здійснюють систематично та широкомасштабно. Опрацювання персональних даних не можна вважати широкомасштабним, якщо опрацювання стосується персональних даних пацієнтів або клієнтів, які надає персональний лікар, інший медичний працівник або юрист. У таких випадках проведення оцінювання впливу на захист даних є необов'язковим.

(92) За деяких обставин, доцільним і раціональним для предмету 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 сектору чи сегменту промисловості або для горизонтальної діяльності широкої сфери застосування.

(93) У контексті ухвалення нормативно-правового акту держави-члена, 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 до початку опрацювання даних.

(94) Якщо у ході оцінювання впливу на захист даних виявляється, що опрацювання, за відсутності гарантій, заходів безпеки та механізмів зниження ризику, створить високий ризик для прав і свобод фізичних осіб, і контролер вважає, що ризик не можна знизити розумними засобами з огляду на наявну технологію та витрати на реалізацію, необхідно провести консультацію з наглядовим органом до початку опрацювання даних. Такий високий ризик, імовірно, є результатом окремих типів опрацювання даних, масштабів і періодичності опрацювання, що може також призвести до нанесення шкоди чи втручання в права та свободи фізичної особи. Наглядовий орган повинен відповісти на запит щодо консультації протягом визначеного строку. Проте відсутність реакції наглядового органу протягом такого строку не повинна обмежувати втручання наглядового органу згідно з його завданнями та повноваженнями, встановленими цим Регламентом, в тому числі, повноваженням забороняти операції опрацювання. Як частину такого консультаційного процесу, результати оцінювання впливу на захист даних, проведеного у зв'язку з відповідним опрацюванням, можна подати до наглядового органу, а саме, інформацію щодо заходів, передбачених для зниження ризику для прав і свобод фізичних осіб.

(95) Оператор повинен надавати допомогу контролеру, за необхідності та на запит, у забезпеченні відповідності зобов'язанням, що виникають в результаті проведення оцінювань впливу на захист даних та попередньої консультації з наглядовим органом.

(96) Консультацію наглядового органу необхідно також проводити під час підготування законодавчого чи регуляторного інструменту, що передбачає опрацювання персональних даних, для того, щоб забезпечити відповідність призначеного опрацювання цьому Регламенту та, зокрема, знизити ризик для суб'єкта даних.

(97) Якщо опрацювання здійснює орган публічної влади, окрім судів або незалежних судових органів, що діють як судові органи, якщо, в приватному секторі, опрацювання здійснює контролер, основні види діяльності якого становлять операції опрацювання, які 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, що

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 необхідний рівень експертних знань, зокрема, відповідно до здійснюваних операцій опрацювання та необхідного захисту для опрацювання персональних даних контролером або оператором. Такі 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 особливі характеристики опрацювання, яке проводять в окремих секторах, а також — особливі потреби мікропідприємств, малих і середніх підприємств. Зокрема, такі кодекси поведінки можуть врегулювати обов'язки контролерів і операторів із врахуванням ризику, що ймовірно виникає внаслідок опрацювання, для прав і свобод фізичних осіб.

(99) Під час розроблення кодексу поведінки або внесення змін до такого кодексу чи його розширення, асоціації та інші органи, що представляють категорії контролерів або операторів, повинні проводити консультації з відповідними стейкхолдерами, в тому числі суб'єктами даних, за можливості, та враховувати отримані матеріали та позиції, висловлені у відповідь на такі консультації.

(100) Для посилення прозорості та відповідності цьому Регламенту необхідно заохочувати запровадження механізмів сертифікації та штампів і знаків захисту даних, що дозволятимуть суб'єктам даних швидко оцінювати рівень захисту даних відповідних продуктів і сервісів.

(101) Потоки персональних даних до країн та з країн поза межами Союзу та міжнародних організацій є необхідними для розширення міжнародної торгівлі та міжнародної співпраці. Зростання таких потоків обумовило нові виклики та занепокоєння у сфері захисту персональних даних. Проте, якщо персональні дані передаються з Союзу до контролерів, операторів або 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 подальших актів передавання персональних даних із третьої країни чи міжнародної організації до контролерів, операторів у тій самій чи іншій третій країні чи міжнародній організації. У будь-якому разі акти передавання до третіх країн та міжнародних організацій можна здійснювати лише за повної відповідності цьому Регламенту. Передавання може мати місце лише у разі, якщо згідно з іншими положеннями цього Регламенту, контролер або оператор дотримуються умов, встановлених у положеннях цього Регламенту щодо передавання персональних даних до третіх країн або міжнародних організацій.

(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, доки такі угоди не впливають на цей Регламент або будь-які інші положення законодавства Союзу та передбачають належний рівень захисту для фундаментальних прав суб'єктів даних.

(103) Комісія може ухвалити рішення, дія якого поширюється на весь Союз про те, що третя країна, територія чи визначений сектор у межах третьої країни, або міжнародна організація забезпечує належний рівень захисту даних, таким чином гарантуючи правову визначеність і 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 такої третьої країни чи міжнародної організації можуть відбуватися без потреби отримання подальшого дозволу. Комісія

може також ухвалити рішення, повідомивши та надавши повний звіт із викладенням причин для третьої країни чи міжнародної організації про скасування такого рішення.

(104) У світлі фундаментальних цінностей, на яких засновано Союз, зокрема, захисту прав людини, Комісія повинна, у своїй оцінці третьої країни чи території або визначеного сектору в межах третьої країни, враховувати те, як певна третя країна поважає верховенство права, доступ до правосуддя, а також міжнародні норми та стандарти прав людини і її загальне та секторальне право, в тому числі законодавство щодо громадської безпеки, оборони та національної безпеки, а також публічний порядок і кримінальне право. Під час ухвалення рішення про відповідність щодо території чи визначеного сектору в третій країні необхідно враховувати чіткі та об'єктивні критерії, такі як спеціальні види опрацювання даних та масштаб застосовних правових стандартів, а також — чинне законодавство в третій країні. Третя країна повинна надати гарантії, що забезпечують належний рівень захисту, який суттєво відповідає тому, що забезпечується 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 із захисту даних держав-членів, а суб'єктам даних — надати дієві права, які можна реалізувати, та дієві адміністративні і судові засоби правового захисту.

(105) Крім міжнародних зобов'язань, що взяли на себе третя країна чи міжнародна організація, Комісія повинна брати до уваги 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. Зокрема, необхідно враховувати приєднання третьої країни до Конвенції Ради Європи про захист фізичних осіб у зв'язку з автоматизованим опрацюванням персональних даних від 28 січня 1981 року та її додаткових протоколів. Комісія повинна провести консультації з радою, оцінюючи рівень захисту в третіх країнах або міжнародних організаціях.

(106) Комісія повинна відстежувати дієвість рішень щодо рівня захисту в третій країні, на території або у визначеному секторі в межах третьої країни, або міжнародній організації та відстежувати дієвість рішень, ухвалених на підставі статті 25(6) або статті 26(4) Директиви 95/46/ЄС. У своїх рішеннях про відповідність, Комісія повинна передбачити механізм періодичної перевірки їхньої дієвості. Таку періодичну перевірку необхідно проводити під час консультації з відповідною третьою країною чи міжнародною організацією, в ній необхідно врахувати всі відповідні розробки в третій країні чи міжнародній організації. Для цілей моніторингу та проведення періодичних перевірок, Комісія повинна враховувати думки та висновки Європейського Парламенту і Ради, а також інших відповідних органів і джерел. Комісія повинна оцінювати, протягом розумного строку, дієвість останніх рішень і звітувати про будь-які відповідні висновки до Комісії у значенні Регламенту Європейського Парламенту і Ради (ЄС) № 182/2011 ([1]), як встановлено цим Регламентом, до Європейського Парламенту і Ради.

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

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

(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 повинні забезпечувати відповідність вимогам щодо 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 адміністративних домовленостей, таких як меморандум про взаєморозуміння, що передбачають права, які можна реалізувати, та дієві права для суб'єктів даних. Необхідно отримати дозвіл компетентного наглядового органу у випадку, якщо гарантії передбачено адміністративними домовленостями, що не мають зобов'язальної сили.

(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 більш всебічний договір, такий як договір між оператором і іншим оператором, ані від додавання інших положень або додаткових гарантій 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 через договірні зобов'язання, що доповнюють стандартні положення про захист.

(110) Група підприємств або група підприємств, що здійснюють спільну господарську діяльність, повинні мати можливість застосовувати зобов'язальні корпоративні правила для здійснення ними міжнародного передавання з Союзу до організацій у межах тієї самої групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, за умови, що такі корпоративні правила містять 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, коли передавання призначене для окремого випадку а є необхідною у зв'язку з договором або судовим позовом, незалежно від того, чи здійснюють його у порядку судової процедури, або в адміністративному чи будь-якому позасудовому порядку, в тому числі в рамках процедур регуляторних органів. Необхідно також передбачити можливість передавання у випадку, коли цього вимагають важливі підстави суспільного інтересу, 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 повинне поширюватися на всі персональні дані чи всі категорії даних, що містяться в реєстрі, 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 відступи 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, що займаються питаннями соціального забезпечення або 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 інтерес, що є істотним для життєво важливих інтересів 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, для важливих цілей 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 є фізично чи юридично неспроможним 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 необхідним для важливих цілей суспільного інтересу або через те, що це відповідає життєво важливим інтересам суб'єкта даних.

(113) Передавання, яке можна кваліфікувати таким, що не повторюється і стосується лише обмеженої кількості суб'єктів даних, є також призначеним для цілей суттєвих законних інтересів 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 надавати відповідні гарантії для захисту фундаментальних прав і свобод фізичних осіб у зв'язку з опрацюванням їхніх персональних даних. Таке передавання повинно бути можливим лише в залишкових випадках, коли жодна з інших підстав для передавання не є застосовною. Для цілей наукового, історичного дослідження або статистичних цілей необхідно брати до уваги правомірні очікування суспільства щодо підвищення рівня знань. Контролер повинен повідомити наглядовий орган та 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, які 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, що перебувають під юрисдикцією держав-членів. Це може 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, що є чинною для третьої країни, яка подає запит, і Союзом або державою-членом. Екстериторіальна сфера застосування таких законів, регламентів та інших нормативно-правових актів може порушувати міжнародне право та може ускладнювати досягнення цілей захисту фізичних осіб, який гарантовано в Союзі цим Регламентом. Дозволено здійснювати лише передавання, під час якого дотримуються умови цього Регламенту щодо передавання до третіх країн. Це може мати місце, між іншим, коли розкриття є необхідним для важливих цілей суспільного інтересу, визнаних законодавством Союзу чи держави-члена, сфера застосування якого поширюється на контролера.

(116) Якщо персональні дані перетинають кордони за межами Союзу, це може викликати підвищений ризик для здатності фізичних осіб реалізовувати права щодо захисту даних,

зокрема, для захисту від незаконного використання чи розкриття такої інформації. Водночас, наглядові органи можуть встановити, що вони неспроможні розглядати скарги чи проводити розслідування, що стосуються видів діяльності, які здійснюють поза їхніми кордонами. Їхні зусилля співпрацювати в транскордонному контексті можуть також ускладнюватися недостатніми запобіжними чи виправними повноваженнями, непослідовними нормативно-правовими режимами та практичними перешкодами, такими як недостатність ресурсів. Таким чином, існує потреба в сприянні тісної співпраці між органами, що здійснюють нагляд за захистом даних, щоб допомогти їм в обміні інформацією та проведенні розслідувань з їхніми міжнародними партнерами. Для цілей розроблення механізмів міжнародної співпраці для сприяння та надання взаємної міжнародної допомоги в забезпеченні виконання положень законодавства щодо захисту персональних даних, Комісія та наглядові органи повинні обмінюватися інформацією та співпрацювати у ході діяльності, пов'язаної з реалізацією їхніх повноважень, з компетентними органами в третіх країнах, за принципом взаємності та згідно з цим Регламентом.

(117) Заснування наглядових органів у державах-членах, наділених правом виконувати свої завдання та реалізовувати свої повноваження у повній незалежності, є істотним компонентом захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних. Держави-члени повинні мати можливість заснувати декілька наглядових органів з метою відображення їхньої конституційної, організаційної та адміністративної структури.

(118) Незалежність наглядових органів не повинна означати те, що наглядові органи не можуть підлягати дії механізмів контролю чи моніторингу щодо їхніх фінансових витрат 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. Така держава-член повинна, зокрема, призначити наглядовий орган, що діятиме як єдиний координаційний центр для результативної участі таких органів у механізмі, щоб забезпечити оперативну та безперервну співпрацю з іншими наглядовими органами, радою і Комісією.

(120) Кожному наглядовому органу необхідно надати фінансові та людські ресурси, приміщення та інфраструктуру, необхідні для результативного виконання 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 частиною загальнодержавного або національного бюджету.

(121) Загальні умови для члена чи членів наглядового органу необхідно встановлювати у законодавчому порядку в кожній державі-члені; зокрема, вони повинні гарантувати призначення таких членів на основі прозорої процедури, парламентом, урядом або главою держави в державі-члені на підставі пропозиції, внесеної урядом, членом уряду, парламентом або палатою парламенту, або незалежним органом, наділеним такими повноваженнями відповідно до законодавства держави-члена. Для забезпечення незалежності наглядового органу, член або члени повинні діяти добросовісно, утримуватися від будь-якої дії, що є несумісною з іншими їхніми обов'язками, та не повинні, протягом строку їхніх повноважень, займатися будь-якою несумісною діяльністю, прибутковою чи ні. Наглядовий орган повинен мати свій власний персонал, відібраний наглядовим органом або незалежним органом, заснованим за законодавством держави-члена, який повинен підпорядковуватися безпосередньому керівництву члена чи членів наглядового органу.

(122) Кожний наглядовий орган повинен володіти компетенцією на території своєї держави-члена для реалізації повноважень та виконання завдань, покладених на нього згідно з цим Регламентом. Вона повинна охоплювати, зокрема, опрацювання в контексті діяльності осідку контролера або оператора на території своєї власної держави-члена,

опрацювання персональних даних, що здійснюють публічні органи чи публічні органи, що діють в цілях суспільного інтересу, опрацювання, яке впливає на суб'єктів даних на його території чи опрацювання, що здійснює контролер або оператор, які не мають осідку в Союзі, коли його спрямовано на суб'єктів даних, що проживають на його території. Це повинно включати розгляд скарг, поданих суб'єктом даних, проведення розслідувань щодо застосування цього Регламенту та сприяння громадській обізнаності про ризики, правила, гарантії та права в зв'язку 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 фізичних осіб у зв'язку з опрацюванням їхніх персональних даних і сприяти вільному потоку персональних даних у межах внутрішнього ринку. З цією метою наглядові органи повинні співпрацювати один з одним і з Комісією, без 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 в більше ніж одній державі-члені, або якщо опрацювання, що відбувається в контексті діяльності єдиного осідку контролера або 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 чи 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. У межах своїх завдань щодо видання настанов з будь-якого питання, що охоплює застосування цього Регламенту, 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 компетентним в ухваленні зобов'язальних рішень щодо заходів із застосування повноважень, покладених на нього згідно з цим Регламентом. Як керівний орган, наглядовий орган повинен активно залучати та координувати наглядові органи, залучені в процесі вироблення й ухвалення рішень. Якщо рішення полягає у відхиленні скарги, поданої суб'єктом даних, повністю або частково, таке рішення повинен ухвалити наглядовий орган, до якого було подано скаргу.

(126) Рішення необхідно узгоджувати у співпраці керівного наглядового органу і відповідних наглядових органів та направляти його до головного або єдиного осідку контролера або оператора, воно повинно бути зобов'язальним для контролера або оператора. Контролер або оператор повинні вживати необхідних заходів для забезпечення відповідності цьому Регламенту та виконання рішення, про яке керівний наглядовий орган повідомив в головний осідок контролера або оператора щодо опрацювання даних в Союзі.

(127) Кожний наглядовий орган, що не діє як керівний наглядовий орган, повинен бути компетентним у розгляді місцевих справ, якщо контролер або оператор мають осідки в більше ніж одній державі-члені, а предмет спеціального опрацювання стосується лише опрацювання, що здійснюють в єдиній державі-члені із залученням лише суб'єктів даних такої єдиної держави-члена, наприклад, якщо предмет стосується опрацювання персональних даних працівників у спеціальному контексті зайнятості в рамках держави-члена. У таких випадках наглядовий орган повинен повідомляти керівний наглядовий орган без затримки щодо суті питання. Після того, як його повідомили, керівний наглядовий орган повинен вирішити, чи розглядатиме він справу відповідно до

положення про співпрацю між керівним наглядовим органом та іншими відповідними наглядовими органами (механізм «єдиного вікна»), або чи повинен наглядовий орган, який про це повідомив, розглядати справу на місцевому рівні. Під час прийняття рішення про те, чи буде він розглядати справу, керівний наглядовий орган повинен взяти до уваги, чи має контролера або оператора осідок в державі-члені наглядового органу, який про це повідомив, для забезпечення результативного виконання рішення щодо контролера або оператора. Якщо керівний наглядовий орган вирішує розглядати справу, наглядовий орган, який повідомив про неї, повинен мати можливість подати проект рішення, на який керівний наглядовий орган повинен звернути максимальну увагу під час підготування свого проекту рішення в рамках 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 цілей суспільного інтересу. У таких випадках єдиним наглядовим органом, компетентним здійснювати повноваження, покладені на нього згідно з 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 повинні мати в кожній державі-члені 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 та брати участь у судовому процесі. Такі повноваження повинні також включати повноваження накладати тимчасове або остаточне обмеження, в тому числі заборону, на опрацювання. Держави-члени мають право визначати інші завдання, пов’язані з захистом персональних даних за цим Регламентом. Повноваження наглядових органів необхідно реалізовувати відповідно до належних процедурних гарантій, встановлених законодавством Союзу та держави-члена, неупереджено, правомірно та в розумний строк. Зокрема, кожний 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 до вжиття будь-якого індивідуального заходу, що негативно вплине на неї, та уникати зайвих витрат і надмірних незручностей для відповідних осіб. Слідчі повноваження щодо доступу до приміщень необхідно реалізовувати відповідно до спеціальних вимог процесуального права держави-члена, зокрема, вимоги щодо отримання попереднього судового дозволу. Кожний юридично зобов’язальний інструмент наглядового органу необхідно оформлювати у письмовій формі, чітко й однозначно, із зазначенням наглядового органу, який ухвалив інструмент, дати ухвалення інструменту, він повинен містити підпис голови чи члена наглядового органу, уповноваженого ним, обґрунтування інструменту, а також повинен вказувати на право щодо дієвого засобу правового захисту. Це не виключає можливість 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 було подано скаргу, не є керівним наглядовим органом, керівний наглядовий орган повинен тісно співпрацювати з наглядовим органом, до якого було подано скаргу, згідно з положеннями щодо співпраці та послідовності, встановленими в цьому Регламенті. У таких випадках керівний наглядовий орган повинен, вживаючи заходів, спрямованих на породження правових наслідків, у тому числі накладення адміністративних штрафів, звертати максимальну увагу на думку наглядового органу, до якого було подано скаргу та який повинен зберігати компетентність у проведенні будь-якого розслідування на території своєї власної держави-члена у взаємодії з компетентним наглядовим органом.

(131) Якщо інший наглядовий орган повинен діяти як керівний наглядовий орган щодо опрацювання даних, яке здійснює оператор або процесор, але конкретний предмет скарги чи можливе порушення стосується лише опрацювання даних, яке здійснює оператор або процесор у державі-члені, де скаргу було подано або можливе порушення було виявлене, а справа не впливає істотно чи ймовірно істотно не впливатиме на суб'єктів даних у інших державах-членах, у такому разі наглядовий орган, що отримує скаргу чи виявляє ситуацію або якого повідомляють іншим чином про ситуації, що тягнуть за собою можливі порушення цього Регламенту, повинен прагнути укладення мирової угоди з контролером і, якщо це виявляється невдалим, реалізувати повний спектр його повноважень. Це включає: спеціальне опрацювання, що здійснюють на території держави-члена наглядового органу чи щодо суб'єктів даних на території тієї держави-члена; опрацювання, що здійснюють в контексті пропонування товарів або послуг, що спеціально призначені для суб'єктів даних на території держави-члена наглядового органу; чи опрацювання, що має бути оцінено, виходячи з відповідних встановлених законом зобов'язань за законодавством держави-члена.

(132) Діяльність щодо підвищення рівня обізнаності громадськості, яку здійснюють 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 своїх завдань та надавати взаємну допомогу для того, щоб забезпечити послідовне застосування та виконання цього Регламенту на внутрішньому ринку. Наглядовий орган, що надсилає запит про взаємну допомогу, може ухвалювати застосування тимчасового інструменту, якщо не отримує відповіді на запит про взаємну допомогу протягом одного місяця з дати отримання такого запиту іншим наглядовим органом.

(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 для співпраці між наглядовими органами. Такий механізм необхідно, зокрема, застосовувати, 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 застосувати, якщо будь-який відповідний наглядовий орган або Комісія надсилає запит про те, що таку справу необхідно розглядати згідно з механізмом послідовності. Такий механізм не повинен обмежувати будь-які заходи, які Комісія може вживати під час реалізації своїх повноважень 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 ухвалювати юридично зобов'язальні рішення в разі суперечок між наглядовими органами. З цією метою вона повинна ухвалювати, як правило, більшістю в дві третини голосів її членів, юридично зобов'язальні рішення в чітко визначених ситуаціях, якщо є суперечливі думки наглядових органів, зокрема, в механізмі послідовності між керівним наглядовим органом і відповідними наглядовими органами по суті справи, зокрема щодо наявності порушення цього Регламенту.

(137) Може виникнути нагальна потреба діяти з метою захисту прав та свобод суб'єктів даних, зокрема якщо існує загроза того, що реалізація права суб'єкта даних може бути істотно ускладненою. Наглядовий орган повинен, таким чином, бути спроможним ухвалювати застосування належним чином обґрунтованих тимчасових інструментів на своїй території з визначеним строком дії, що не повинен перевищувати три місяці.

(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 між керівним наглядовим органом і відповідними наглядовими органами, а надання взаємної допомоги і здійснення спільних операцій може відбуватися між відповідними наглядовими органами на двосторонній чи багатосторонній основі без застосування механізму послідовності.

(139) Для того, щоб сприяти послідовному застосуванню цього Регламенту, раду необхідно заснувати як незалежний орган Союзу. Для досягнення своїх цілей, рада повинна володіти правосуб'єктністю. Раду повинен представляти її Голова. Вона повинна замінити Робочу групу із захисту осіб у сфері опрацювання персональних даних, засновану Директивою 95/46/ЄС. Вона повинна складатися з голови наглядового органу кожної держави-члена та Європейського інспектора із захисту даних або їхніх відповідних представників. Комісія повинна брати участь в діяльності ради без права голосу, а Європейський інспектор із захисту даних повинен мати особливе право голосу. Рада повинна 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 в межах Союзу. Рада повинна діяти незалежно під час виконання своїх завдань.

(140) Раді повинен 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 його постійного проживання, та право на дієві засоби судового захисту згідно зі статтею 47 Хартії, якщо суб'єкт даних вважає, що його або її права за цим Регламентом було порушено, або якщо наглядовий орган не розглядає скаргу, частково чи повністю відхиляє або відмовляє в розгляді скарги, або демонструє бездіяльність у разі необхідності вжити відповідних заходів для захисту прав суб'єкта даних. Після отримання скарги необхідно провести 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. Щоб полегшити подання скарг, кожний наглядовий орган повинен вживати заходів, наприклад, надання форми подання скарги, яку також можна оформити в електронному форматі, без обмеження 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, засновані за законодавством держави-члена, які мають статутні цілі у сфері суспільних інтересів та здійснюють активну діяльність в 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 в результаті 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 статтею 263 ДФЄС. Як адресати таких рішень,

зацікавлені наглядові органи, що бажають їх оскаржити, повинні подати позов протягом двох місяців після того, як їх було повідомлено про них, згідно зі статтею 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 статтею 263 ДФЄС. Без обмеження цього права відповідно до статті 263 ДФЄС, кожна фізична чи юридична особа повинна мати дієвий засіб судового захисту в компетентному національному суді щодо рішення наглядового органу, що 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 необхідно здійснювати в судах держави-члена, де засновано наглядовий орган, та відповідно до процесуального права тієї держави-члена. Такі суди повинні здійснювати повну юрисдикцію, що охоплює юрисдикцію щодо розгляду всіх питань факту та права, які стосуються відповідного спору.

У разі відмови у задоволенні скарги чи її відхилення з боку наглядового органу, заявник може звернутися до судів тієї самої держави-члена. У контексті засобів судового захисту, що стосуються застосування цього Регламенту, національні суди, що розглядають рішення з питання, необхідного для надання їм повноваження винести рішення, можуть, або у випадку, передбаченому статтею 267 ДФЄС, повинні, надіслати запит до Суду про винесення попередньої ухвали щодо тлумачення нормативно-правового акту Союзу, в тому числі цього Регламенту. Більш того, якщо рішення наглядового органу, на основі якого здійснюють виконання рішення ради, оскаржують в національному суді, а законність рішення ради є спірною, такий національний суд не має повноваження оголошувати рішення ради незаконним, але повинен передати питання щодо законності до Суду згідно зі статтею 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 особисто її, але не зробила цього протягом строку, встановленого в статті 263 ДФЄС.

(144) Якщо суд, який розпочав провадження щодо рішення наглядового органу, має підстави вважати, що провадження щодо того самого опрацювання, зокрема, того самого предмету, 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 їхній спільний розгляд та вирішення стає доцільним для уникнення ризику ухвалення суперечливих рішень, винесених у рамках 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 — де проживає суб'єкт даних, за винятком, якщо контролер є публічним органом держави-члена, що виконує свої публічні повноваження.

(146) Контролер або оператор повинні відшкодувати будь-яку шкоду, заподіяну особі в результаті опрацювання із порушенням цього Регламенту. Контролера або оператора

необхідно звільнити від відповідальності у разі доведення, 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 акту 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, що уточнює норми цього Регламенту. Суб'єкти даних повинні отримати повне та результативне відшкодування за заподіяну їм шкоду. У випадку залучення контролерів або операторів до того самого опрацювання, кожний контролер або оператор повинен нести відповідальність за нанесення шкоди у повному обсязі. Проте, у разі їхньої спільної участі в одному провадженні, згідно із законодавством держави-члена, відшкодування може бути розподілено з урахуванням відповідальності кожного контролера або оператора за шкоду, заподіяну внаслідок опрацювання, за умови забезпечення в повному обсязі результативного відшкодування суб'єкту даних, якому було 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 ([1]), не повинні обмежувати застосування таких спеціальних норм.

(148) З метою посилення ступеня застосування норм цього Регламенту, санкції, в тому числі, адміністративні штрафи, необхідно накладати за будь-яке порушення цього Регламенту, окрім або замість відповідних заходів, застосованих наглядовим органом відповідно до цього Регламенту. У разі незначного порушення або якщо штраф, який ймовірно буде накладено, становитиме надмірний тягар для фізичної особи, 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-який інший обтяжувальний або пом'якшувальний фактор. На накладення штрафів, у тому числі адміністративних штрафів, повинні поширюватися відповідні процесуальні гарантії згідно із загальними принципами законодавства Союзу та Хартії, в тому числі дієвий судовий захист та належна правова процедура.

(149) Держави-члени повинні мати можливість встановлювати норми щодо кримінальних покарань за порушення цього Регламенту, в тому числі за порушення національних норм, ухвалених відповідно до та з урахуванням обмежень цього Регламенту. Такі кримінальні покарання можуть також допускати позбавлення переваг, отриманих внаслідок порушення цього Регламенту. Проте призначення кримінальних покарань за порушення таких національних правил та адміністративних санкцій не повинні призводити до порушення принципу *ne bis in idem*, як його тлумачить Суд.

(150) Щоб посилити та гармонізувати адміністративні санкції за порушення цього Регламенту, кожний наглядовий орган повинен мати повноваження накладати адміністративні штрафи. Цей Регламент повинен зазначати порушення і верхню межу та критерії встановлення пов'язаних адміністративних штрафів, які повинен визначити компетентний наглядовий орган у кожному окремому випадку, беручи до уваги всі

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

відповідні обставини конкретної ситуації, з належним врахуванням, зокрема, специфіки, тяжкості, тривалості порушення і його наслідків та інструментів, що було застосовано для забезпечення відповідності обов'язкам за цим Регламентом та запобігання чи пом'якшення наслідків порушення. Якщо адміністративні штрафи було накладено на підприємство, його необхідно розуміти як підприємство згідно зі статтями 101 і 102 ДФЄС для цих цілей. Якщо адміністративні штрафи було накладено на осіб, що не є підприємством, наглядовий орган повинен враховувати загальний рівень доходу в державі-члені, а також економічну ситуацію особи, під час визначення необхідного рівня штрафу. Механізм послідовності також можна використовувати для сприяння послідовному застосуванню адміністративних штрафів. Саме держави-члени мають визначити, чи повинні органи публічної влади підлягати накладенню адміністративних штрафів та якою мірою. Накладення адміністративного штрафу чи попередження не впливає на застосування інших повноважень наглядових органів або інших санкцій за цим Регламентом.

(151) Правовими системами Данії та Естонії не передбачено накладення адміністративних штрафів, як встановлено 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 в рамках процедури незначних правопорушень, за умови, що таке застосування правил у таких державах-членах має наслідки, аналогічні накладенню адміністративних штрафів наглядовими органами. Тому, компетентні національні суди повинні враховувати рекомендацію наглядового органу, який порушує питання щодо 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, повинно визначати законодавство держави-члени.

(153) Держави-члени повинні узгоджувати норми, що регулюють свободу вияву поглядів та 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 дія відступів чи винятків від деяких положень цього Регламенту, якщо це необхідно для узгодження права на захист персональних даних із правом на свободу вияву поглядів та свободу інформації, як закріплено в статті 11 Хартії. Це необхідно застосовувати, зокрема, до 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 цих фундаментальних прав. Держави-члени повинні ухвалити такі винятки і відступи щодо загальних принципів, прав суб'єкта даних, контролера і оператора, передавання персональних даних до третіх країн чи міжнародних організацій, незалежних наглядових органів, співпраці і послідовності, та спеціальних ситуацій з опрацювання даних. Якщо такі винятки чи відступи відрізняються в декількох державах-членах, необхідно застосовувати законодавство держави-члени, яке поширюється на контролера. Щоб врахувати важливість права на свободу вияву поглядів у кожному демократичному суспільстві, поняття такої свободи, наприклад в журналістиці, необхідно тлумачити у широкому сенсі.

(154) Цей Регламент передбачає врахування принципу публічного доступу до офіційних документів під час застосування цього Регламенту. 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 передбачено законодавством Союзу чи держави-члена, яке поширюється на публічний орган чи організацію. Таке законодавство повинно узгодити питання публічного доступу до офіційних документів та повторного використання інформації публічної сфери із правом на захист персональних даних і може, відтак, передбачати необхідне 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 яких поширюється сфера дії законодавства держави-члена про публічний доступ до документів. Директива Європейського Парламенту і Ради 2003/98/ЄС ([1]) залишає без змін і жодним чином не впливає на рівень захисту фізичних осіб у зв'язку з опрацюванням персональних даних згідно з 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 було передбачено на законодавчому рівні як таке, що є несумісним 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», може 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 організацію праці, рівність та різноманітність на робочому місці, здоров'я та безпеку 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 досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей повинно підлягати застосуванню відповідних гарантій для прав і свобод суб'єкта даних відповідно до цього Регламенту. Такі гарантії повинні забезпечувати наявність технічних і організаційних інструментів для гарантування, зокрема, принципу мінімізації даних. Подальше опрацювання персональних даних для досягнення 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 ідентифікацію суб'єктів даних, за умови, що існують відповідні гарантії (такі як, наприклад, використання псевдонімів до даних). Держави-члени повинні передбачити відповідні гарантії для опрацювання персональних даних для досягнення цілей суспільних інтересів, цілей наукового і історичного дослідження або статистичних цілей. Держав-членів необхідно уповноважити надавати, за спеціальних умов і з урахуванням відповідних гарантій для суб'єктів даних, уточнення та відступи, що стосуються вимог до інформації та прав на виправлення, стирання, права бути забутим, обмеження опрацювання, мобільності даних і заперечення, коли опрацьовують персональні дані для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей. Відповідні умови та гарантії можуть тягти за собою спеціальні процедури для суб'єктів даних для реалізації таких прав, 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

([1]) Директива Європейського Парламенту і Ради 2003/98/ЄС від 17 листопада 2003 року про повторне використання інформації публічного сектора (ОВ L 345, 31.12.2003, с.90).

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 широко розповсюджених медичних станів, таких як серцево-судинне захворювання, рак і депресія. На підставі реєстрів можна посилити результати досліджень, оскільки вони охоплюють більшу кількість населення. У суспільній науці дослідження на підставі реєстрів дає можливість дослідникам отримати необхідні знання про довготривалий взаємозв'язок певної кількості суспільних умов, таких, як безробіття та освіта, з іншими життєвими умовами. Результати дослідження, отримані через реєстри, надають міцні, високоякісні знання, що можуть становити основу для розроблення та реалізації політики, заснованої на знаннях, покращити якість життя для певної кількості людей і підвищити ефективність постачання соціальних послуг. Сприяючи науковому дослідженню, персональні дані можна опрацьовувати для цілей наукового дослідження, за дотримання відповідних умов і гарантій, встановлених законодавством Союзу чи держави-члена.

(158) Якщо персональні дані опрацьовують для архівних цілей, цей Регламент необхідно застосовувати до такого опрацювання, враховуючи, що цей Регламент не застосовують до померлих осіб. Публічними органами або публічними чи приватними органами, що ведуть записи суспільного інтересу, повинні бути служби, що, згідно з законодавством Союзу чи держави-члена, мають встановлене законом зобов'язання 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 забезпечення подальшого опрацювання персональних даних для цілей архівації, наприклад, для надання спеціальної інформації, що стосується політичної поведінки в умовах колишніх режимів тоталітарних держав, геноциду, злочинів проти людяності, зокрема, Голокосту, або воєнних злочинів.

(159) Якщо персональні дані опрацьовують для цілей наукових досліджень, цей Регламент необхідно також застосовувати до такого опрацювання. В рамках цього Регламенту, опрацювання персональних даних для цілей наукового дослідження необхідно тлумачити в широкому сенсі, у тому числі, наприклад, в аспекті технологічних розробок і демонстрації, фундаментального дослідження, прикладного дослідження і дослідження за фінансової підтримки з боку приватного сектору. Крім того, необхідно брати до уваги мету Союзу, відображену в статті 179(1) ДФЄС щодо формування Європейського дослідницького простору. Цілі наукового дослідження повинні також включати навчання, що проводять в суспільних інтересах у сфері охорони суспільного здоров'я. Зважаючи на особливості характеристики опрацювання персональних даних для цілей наукового дослідження, необхідно застосовувати спеціальні умови, зокрема, в тому, що стосується опублікування чи іншого розкриття персональних даних у контексті цілей наукового дослідження. Якщо результат наукового дослідження, зокрема, в контексті здоров'я надає підстави для вжиття подальших заходів в інтересах суб'єкта даних, необхідно застосувати загальні норми цього Регламенту на підставі таких заходів.

(160) Якщо персональні дані опрацьовують для цілей історичних досліджень, цей Регламент необхідно також застосовувати до такого опрацювання. Це також передбачає історичне дослідження і дослідження для генеалогічних цілей, зважаючи на те, що 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 ([1]).

(162) Якщо персональні дані опрацьовують для статистичних цілей, цей Регламент необхідно також застосовувати до такого опрацювання. У законодавстві Союзу чи держави-члена необхідно, в межах цього Регламенту, визначити статистичний зміст, контроль за доступом, особливості опрацювання персональних даних для статистичних цілей, відповідні заходи для захисту прав і свобод суб'єкта даних та забезпечення статистичної конфіденційності. Статистичні цілі означають будь-яку операцію щодо збирання та опрацювання персональних даних, необхідних для статистичних спостережень або для підготування статистичних результатів. Такі статистичні результати можна надалі використовувати 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) Необхідно захистити конфіденційну інформацію, яку Союз і національні органи статистики збирають для підготування офіційної європейської та офіційної національної статистики. Європейську статистику необхідно розробляти, готувати та розповсюджувати згідно зі статистичними принципами, як встановлено в статті 338(2) ДФЄС, а національну статистику також — відповідно до законодавства держави-члена. Регламент Європейського Парламенту і Ради (ЄС) № 223/2009 ([2]) надає детальні уточнення щодо 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 для охорони професійних зобов'язань або інших рівноцінних зобов'язань щодо конфіденційності мірою необхідності цього для узгодження права на захист персональних даних із обов'язком збереження професійної таємниці. Це не обмежує чинні зобов'язання держави-члена ухвалювати норми щодо професійної таємниці, якщо це необхідно за законодавством Союзу.

(165) Цей Регламент поважає та не обмежує статус церков і релігійних асоціацій чи спільнот за чинним конституційним правом держав-членів, як це визнано у статті 17 ДФЄС.

(166) Для виконання цілей цього Регламенту, а саме, захисту фундаментальних прав і свобод фізичних осіб і, зокрема, їхнього права на захист персональних даних, а також для забезпечення вільного руху персональних даних у всьому Союзі, Комісії необхідно делегувати повноваження ухвалювати акти згідно зі статтею 290 ДФЄС. Зокрема, делеговані акти необхідно ухвалювати на основі критеріїв і вимог для механізмів сертифікації, інформацію необхідно надавати у форматі стандартизованих іконок та процедур для надання таких іконок. Особливо важливим є проведення Комісією відповідних консультації під час своєї підготовчої роботи, в тому числі, — на рівні експертів. Комісія, під час підготування та розроблення делегованих актів, повинна забезпечувати одночасне, вчасне та належне передавання відповідних документів до Європейського Парламенту і Ради.

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

([2]) Регламент Європейського Парламенту і Ради (ЄС) № 223/2009 від 11 березня 2009 року 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).

(167) Для забезпечення єдиних умов імплементації цього Регламенту Комісії необхідно надати виконавчі повноваження, якщо це передбачено цим 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) Необхідно застосовувати експертну процедуру для ухвалення імплементаційних актів щодо стандартних договірних положень між контролерами і операторами та між операторами; кодексів поведінки; технічних стандартів і механізмів сертифікації; належного рівня захисту, що надає третя країна, територія чи спеціальний сектор у межах тієї третьої країни, або міжнародна організація; стандартних положень про захист; форматів і процедур для обміну інформацією електронними засобами між контролерами, операторами та наглядовими органами щодо зобов'язальних корпоративних правил; взаємної допомоги; домовленостей для обміну інформацією електронними засобами між наглядовими органами та між наглядовими органами і радою.

(169) Комісія повинна негайно ухвалити застосовні імплементаційні акти, якщо наявні докази відображають, що третя країна, територія чи спеціальний сектор у межах такої третьої країни, або міжнародна організація не забезпечують належного рівня захисту, та якщо це необхідно невідкладно і терміново.

(170) Оскільки мету цього Регламенту, зокрема щодо забезпечення належного рівня захисту фізичних осіб та вільного потоку 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 відповідно до принципу субсидіарності, як це передбачено в статті 5 Договору про Європейський Союз. Відповідно до принципу пропорційності, встановленого зазначеною статтею, цей Регламент не виходить за межі необхідного для досягнення такої цілі.

(171) Директиву 95/46/ЄС необхідно скасувати цим Регламентом. Опрацювання, що вже було розпочато станом на дату застосування цього Регламенту, необхідно привести у відповідність з цим Регламентом протягом дворічного періоду з дати набуття чинності цим Регламентом. Якщо опрацювання засновано на згоді відповідно до Директиви 95/46/ЄС, немає потреби для суб'єкта даних надавати свою повторну згоду, якщо спосіб, у який було надано згоду, відповідає умовам цього Регламенту, і таким чином дозволяє контролеру продовжувати таке опрацювання після дати застосування цього Регламенту. 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 було проведено консультацію згідно зі статтею 28(2) Регламенту (ЄС) № 45/2001, він надав висновок від 7 березня 2012 року ([1]).

(173) Цей Регламент необхідно застосовувати до усіх питань, 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 ([2]), у тому числі зобов'язань, покладених на контролера, і прав фізичних осіб. Для того, 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 цьому Регламенту,

---

([1]) ОВ С 192, 30.06.2012, с. 7.

([2]) Директива Європейського Парламенту і Ради 2002/58/ЄС від 12 липня 2002 року 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:

ГЛАВА I

Загальні положення

Стаття 1

Предмет і цілі

1. Цей Регламент установлює норми щодо захисту фізичних осіб у зв'язку з опрацюванням персональних даних і норми про вільний рух персональних даних.

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

3. Вільний рух персональних даних у всьому Союзі не повинно бути обмежено чи заборонено із причин, пов'язаних із захистом фізичних осіб у зв'язку з опрацюванням персональних даних.

Стаття 2

Матеріальна сфера дії

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

2. Цей Регламент не застосовують до опрацювання персональних даних:

(a) в ході діяльності, що виходить за межі дії права Союзу;

(b) державами-членами під час реалізації діяльності, що виходить за межі глави 2 розділу V Договору про ЄС;

(c) фізичною особою під час задоволення особистих або побутових потреб;

(d) компетентними органами 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, що застосовні до такого опрацювання персональних даних, необхідно адаптувати до принципів і правил цього Регламенту відповідно до статті 98.

4. Цей Регламент не перешкоджає застосуванню Директиви 2000/31/ЄС, зокрема, норм щодо відповідальності надавачів послуг, передбачених у статтях 12-15 зазначеної Директиви.

Стаття 3

Територіальна сфера дії

1. Цей Регламент застосовують до опрацювання персональних даних в контексті діяльності осідку контролера або оператора в Союзі, незалежно від того, чи відбувається власне опрацювання в межах Союзу чи ні.

2. Цей Регламент застосовують до опрацювання персональних даних суб'єктів даних, які перебувають у Союзі, контролером або оператором, який має осідок поза межами Союзу, якщо опрацювання даних пов'язано з:

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

(b) моніторингом поведінки суб'єктів даних, якщо така поведінка має місце у межах Союзу.

3. Цей Регламент застосовують до опрацювання персональних даних контролером, що має осідок поза межами Союзу, але в місці, де застосовується законодавство держави-члена в силу публічного міжнародного права.

Стаття 4

Терміни та означення

Для цілей цього Регламенту:

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

(2) «опрацювання» означає будь-яку операцію або низку операцій з персональними даними або наборами персональних даних з використанням автоматизованих засобів або без них, такі 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;

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

(4) «профайлінг» означає будь-яку форму автоматизованого опрацювання персональних даних, що складається із використання персональних даних для оцінювання окремих персональних аспектів, що стосуються фізичної особи, зокрема, для аналізу або прогнозування аспектів, що стосуються продуктивності суб'єкта даних на роботі, економічної ситуації, здоров'я, особистих переваг, інтересів, надійності, поведінки, місцезнаходження або пересування;

(5) «використання псевдонімів» означає опрацювання персональних даних у такий спосіб, що персональні дані більше не можна віднести 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, що персональні дані не віднесено до фізичної особи, яку ідентифіковано чи можна ідентифікувати;

(6) «картотека» означає будь-який структурований набір персональних даних, доступ до якого надають відповідно до спеціальних критеріїв, є централізованим, децентралізованим або розосередженим на функціональній або географічній основі;

(7) «контролер» означає фізичну чи юридичну особу, 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 може бути передбачено законодавством Союзу чи держави-члена;

(8) «оператор» означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, який опрацьовує персональні дані від імені контролера;

(9) «одержувач» означає фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, якому розкривають персональні дані, незалежно від того, чи є вони третьою

стороною. Проте органів публічної влади, що можуть отримувати персональні дані в рамках конкретного запиту згідно з законодавством Союзу чи держави-члена, не вважають одержувачами; опрацювання таких даних такими органами публічної влади повинно відповідати застосовним нормам про захист даних відповідно до цілей опрацювання;

(10) «третя сторона» означає фізичну чи юридичну особу, 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 означає будь-яке вільно надане, конкретне, поінформоване та однозначне зазначення бажань суб'єкта даних, яким він або вона, шляхом оформлення заяви чи проявом чітких ствердних дій, підтверджує згоду на опрацювання своїх персональних даних;

(12) «порушення захисту персональних даних» означає 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» означає персональні дані, що стосуються вроджених або набутих генетичних ознак фізичної особи, надають 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» означають персональні дані, отримані в результаті спеціального технічного опрацювання, що стосується фізичних, фізіологічних чи поведінкових ознак фізичної особи, таких як, зображення обличчя чи дактилоскопічні дані, що дозволяють однозначно ідентифікувати або підтверджують однозначну ідентифікацію фізичної особи;

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

(16) «головний осідок» означає:

(a) щодо контролера, що 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 такі рішення, необхідно вважати головним;

(b) щодо оператора що 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 в контексті діяльності осідку оператора тією мірою, якою на оператора поширюються конкретні обов'язки за цим Регламентом;

(17) «представник» означає фізичну чи юридичну особу, що перебуває чи має осідок в Союзі, та призначена контролером або оператором у письмовій формі згідно зі статтею 27, представляє контролера або оператора у питанні, що стосується їхніх відповідних обов'язків за цим Регламентом;

(18) «підприємство» означає фізичну чи юридичну особу, що займається господарською діяльністю, незалежно від організаційно-правової форми, в тому числі партнерства чи асоціації, що займаються господарською діяльністю на постійній основі;

(19) «група підприємств» означає підприємство, що контролює, і підприємства, що перебувають під його контролем;

(20) «зобов'язальні корпоративні правила» означає політику 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 здійснюють спільну господарську діяльність;

(21) «наглядовий орган» означає незалежний публічний орган, заснований державою-членом відповідно до статті 51;

(22) «відповідний наглядовий орган» означає 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 будуть зазнавати істотного впливу в результаті опрацювання;

(c) до такого наглядового органу було подано скаргу;

(23) «транскордонне опрацювання» означає або:

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

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

(24) «відповідне і вмотивоване заперечення» означає 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 значимість ризиків, що спричиняє проект рішення, для фундаментальних прав і свобод суб'єктів даних та, у відповідних випадках, вільного руху персональних даних в межах Союзу;

(25) «послуга інформаційного суспільства» означає послугу, як її означено в пункті (b) статті 1(1) Директиви Європейського Парламенту і Ради (ЄС) 2015/1535 ([1]);

(26) «міжнародна організація» означає організацію та її підпорядковані органи, що регулюються публічним міжнародним правом, або будь-який інший орган, заснований договором або на основі договору між двома чи декількома державами.

ГЛАВА 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»);

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

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

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

(d) вважати точними і, за необхідності, оновлювати; необхідно вживати усіх відповідних заходів для того, щоб забезпечити, що неточні персональні дані, зважаючи на цілі їхнього опрацювання, було стерто чи виправлено без затримки («точність»);

(e) зберігати в формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це є необхідним для цілей їхнього опрацювання; персональні дані можна зберігати протягом більш тривалих періодів, доки їх опрацьовують винятково для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей відповідно до статті 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 проти несанкціонованого чи незаконного опрацювання та проти ненавмисної втрати, знищення чи завдання 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 вжиття 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 завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера;

(f) опрацювання є необхідним для цілей 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.

Пункт (f) першого підпараграфа не застосовують до опрацювання, яке здійснюють публічні органи у ході виконання своїх завдань.

2. Держави-члени можуть мати або вводити уточнені положення для застосування норм цього Регламенту щодо опрацювання з метою дотримання пунктів (c) і (e) параграфа 1, визначивши більш чітко спеціальні вимоги опрацювання та інші засоби для забезпечення

законного та правомірного опрацювання, в тому числі, для інших спеціальних ситуацій опрацювання, як це передбачено главою IX.

3. Законодавчу базу, вказану в пункті (c) і (e) параграфа 1, визначає:

(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 пункті (e) параграфа 1, її необхідно обов'язково передбачити для виконання завдання в суспільних інтересах чи здійснення офіційних повноважень, покладених на контролера. Така законодавча база може містити спеціальні положення для адаптації застосування правил цього Регламенту, між іншим: 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 щодо забезпечення законного та справедливого опрацювання як ті, що вживають в інших спеціальних ситуаціях опрацювання, як передбачено в главі IX. Законодавство Союзу або держави-члена повинно відповідати меті суспільного інтересу та бути пропорційним наявній законній цілі.

4. Якщо опрацювання для іншої цілі, ніж тієї для якої відбувалося збирання персональних даних, не засновано на згоді суб'єкта даних або на законодавстві Союзу чи держави-члена, що є необхідним і пропорційним заходом у демократичному суспільстві для гарантування цілей, вказаних у статті 23(1), контролер, для того, щоб переконатися, чи є опрацювання для іншої цілі сумісним із ціллю первинного збирання персональних даних, повинен врахувати, між іншим:

(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 контролера;

(c) специфіку персональних даних, зокрема, питання опрацювання спеціальних категорій персональних даних, згідно зі статтею 9, або опрацювання персональних даних про судимості і кримінальні злочини, згідно зі статтею 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. У разі, 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 формі, що чітко відрізняється від інших питань, у зрозумілій та доступній формі, 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 момент. Відкликання згоди не повинно впливати на законність опрацювання, що ґрунтувалося на згоді до її відкликання. До надання згоди суб'єкта даних необхідно про це повідомити. Необхідно однаково забезпечити можливість як відкликати, так і надати згоду.

4. Здійснюючи оцінку того, чи є згода вільно наданою, необхідно максимально враховувати те, чи залежить, між іншим, виконання договору, в тому числі надання послуги, від згоди на опрацювання персональних даних, що не є необхідною для виконання такого договору.

Стаття 8

Умови, застосовні до згоди дитини в сфері послуг інформаційного суспільства

1. У разі застосування пункту (a) статті 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 якщо та тією мірою, коли 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 такий вік не є нижчим 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, з урахуванням наявних технологій.

3. Пункт 1 не впливає на загальне договірне право держав-членів, таке як 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, чи членство в професійних спілках, і 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. Параграф 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, якщо законодавством Союзу чи держави-члена передбачено, що суб'єкт даних не може зняти заборону, вказану в параграфі 1;

(b) опрацювання є необхідним 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 або колективною угодою згідно з законодавством держави-члена, що надає необхідні гарантії для фундаментальних прав та інтересів суб'єкта даних;

(c) опрацювання є необхідним 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 в 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 винятково членів чи колишніх членів органу або до осіб, що регулярно підтримують контакт 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 є необхідним для формування, здійснення або захисту правових претензій або якщо суди діють як судові органи;

(g) опрацювання є необхідним 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 є необхідним для цілей превентивної медицини чи гігієни праці, для оцінювання працездатності працівника, медичного діагнозу, надання послуг у сфері охорони здоров'я чи соціального забезпечення чи лікування або управління системами та послугами в сфері охорони здоров'я чи 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 параграфі 3;

(i) опрацювання є необхідним з причин суспільного інтересу в сфері охорони суспільного 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 є необхідним для досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження або статистичних цілей відповідно до статті 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 параграфі 1, можна опрацьовувати для цілей, зазначених у пункті (h) параграфа 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 або нормами, встановленими національними компетентними органами чи іншою особою також з урахуванням обов'язку збереження таємниці згідно з законодавством Союзу або держави-члена або нормами, встановленими національними компетентними органами.

4. Держави-члени можуть мати або вводити деталізовані умови, в тому числі, обмеження, у зв'язку з опрацюванням генетичних даних, біометричних даних або даних стосовно стану 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 статті 6(1) здійснюють лише під контролем офіційного органу або у разі, якщо опрацювання дозволено законодавством Союзу або 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 параграфі 1 цієї статті, контролер здатний довести, що він не може ідентифікувати суб'єкта даних, контролер, відповідно, за можливості, повинен повідомити про це суб'єкта даних. У таких ситуаціях, статті 15–20 не застосовують, за винятком, якщо суб'єкт даних, з метою реалізації своїх прав за зазначеними статтями, надає додаткову інформацію, що уможливлюють його ідентифікацію.

ГЛАВА 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 статтях 13 і 14 та в будь-якому повідомленні згідно зі статтями 15–22 і 34 щодо опрацювання, суб'єкту даних у стислій, прозорій, доступній для розуміння та легко доступній формі, з використанням чітких і простих формулювань, зокрема, для будь-якої інформації, яку спеціально призначено для дитини. Інформацію необхідно надавати у письмовій формі або іншими засобами, в тому числі, за необхідності, електронними засобами. У разі надання запиту суб'єктом даних, інформацію можна бути надано усно, за умови, що особу суб'єкта даних доведено іншими засобами.

2. Контролер повинен сприяти реалізації прав суб'єктом даних згідно зі статтями 15–22. У випадках, вказаних у статті 11(2), контролер не має права ухилятися від дій на запит суб'єкта даних щодо реалізації його прав за статтями 15–22, за винятком, доведення контролером неможливості ідентифікувати суб'єкта даних.

3. Контролер повинен надати інформацію щодо дії, вжитої на запит за статтями 15–22, суб'єкту даних без необґрунтованої затримки та в будь-якому випадку протягом одного місяця з дати отримання запиту. За необхідності, зважаючи на складність та 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 прохання суб'єкта даних про інше.

4. Якщо контролер не вживає дій 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. Інформацію, що надають за статтями 13 і 14, і будь-яке повідомлення та будь-які дії, яких вживають за статтями 15–22 і 34, необхідно надавати на безоплатній основі. Якщо запити від суб'єкта даних є явно необґрунтованими чи надмірними, зокрема, через їхнє багатократне повторення, контролер може або:

(a) стягнути розумну плату, враховуючи адміністративні витрати на надання інформації або повідомлення чи вжиття дій на запит; або

(b) ухилитися від виконання дій на запит.

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

6. Без обмеження статті 11, якщо контролер має вагомі підстави сумніватися в особистості фізичної особи, що здійснює запит, вказаний у статтях 15–21, контролер може надіслати запит на надання додаткової інформації, необхідної для підтвердження особистості суб'єкта даних.

7. Інформацію, яку необхідно надати суб'єктам даних відповідно до статей 13 і 14, можна надавати в поєднанні зі стандартизованими іконками для того, щоб надати конструктивний огляд призначеного опрацювання у видимий, доступний для розуміння та чіткий спосіб. У випадку електронного представлення іконок, — вони повинні легко зчитуватися машиною.

8. Комісії необхідно надати повноваження ухвалювати делеговані акти згідно зі статтею 92 з метою визначення інформації, необхідної для представлення в іконках, та процедур для 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 збирають від суб'єкта даних, контролер повинен, у момент отримання персональних даних, надати суб'єкту даних усю інформацію, а саме 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) якщо опрацювання здійснюють на підставі пункту (f) статті 6(1), законні інтереси контролера або третьої сторони;

(e) одержувачі 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 статті 46 чи 47, або другому підпараграфі статті 49(1), — зазначення належних чи відповідних гарантій і засобів, за допомогою яких можна отримати копію таких даних, або джерела, звідки їх можна отримати у вільному доступі.

2. Крім інформації, вказаної в параграфі 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, стирання, обмеження опрацювання щодо суб'єкта даних або на заперечення проти опрацювання, а також права на мобільність даних;

(c) якщо опрацювання здійснюють на підставі пункту (a) статті 6(1) або пункту (a) статті 9(2), — існування права на відкликання згоди в будь-який момент, без наслідків для законності опрацювання, що було засновано на згоді до її відкликання;

(d) право подавати скаргу до наглядового органу;

(e) те, чи є надання персональних даних статутною чи 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 статті 22(1) та (4) і, принаймні в таких випадках, достовірної інформації про логіку, значимість та передбачувані наслідки такого опрацювання для суб'єкта даних.

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

4. Параграфи 1, 2 і 3 не застосовують, якщо і 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 було отримано не від суб’єкта даних, контролер повинен надати суб’єкту даних 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) категорії відповідних персональних даних;

(e) одержувачі 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 статті 46 чи 47, або другому підпараграфі статті 49(1), — зазначення належних чи відповідних гарантій і засобів, за допомогою яких можна отримати копію таких даних, або джерела, звідки їх можна отримати 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 пункту (f) статті 6(1), законні інтереси контролера або третьої сторони;

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

(d) якщо опрацювання здійснюють на підставі пункту (a) статті 6(1) або пункту (a) статті 9(2), — існування права на відкликання згоди в будь-який момент, без наслідків для законності опрацювання, що ґрунтувалося на згоді до її відкликання;

(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 статті 22(1) та (4) і, принаймні в таких випадках, достовірної інформації про логіку, значимість та передбачувані наслідки такого опрацювання для суб’єкта даних.

3. Контролер повинен надати інформацію, вказану в параграфах 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 прагне надалі опрацьовувати персональні дані для іншої цілі, ніж та, для якої персональні дані було отримано, контролер повинен надати суб'єкту даних до початку такого подальшого опрацювання інформацію про таку іншу ціль і будь-яку належну детальну інформацію, як вказано в параграфі 2.

5. Параграфи 1–4 не застосовують, якщо і 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 цілях, із урахуванням умов і гарантій, зазначених у статті 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 передбачено 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, статутний обов'язок 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) одержувачі чи категорії одержувача, якому персональні дані були або будуть розкриті, зокрема, одержувачі в 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 стирання 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 збирають від суб'єкта даних, будь-яку інформацію щодо їхнього джерела;

(h) наявність автоматизованого вироблення й ухвалення рішень, у тому числі профайлінгу, вказаного в статті 22(1) та (4) і, принаймні в таких випадках, достовірної інформації про логіку, значимість та 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 статті 46 щодо передавання даних.

3. Контролер повинен надати копію персональних даних, які знаходяться у процесі опрацювання. Для 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 його прохання щодо іншої форми інформацію необхідно надавати загальноприйнятими електронними засобами.

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

Секція 3

Виправлення та стирання

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 заповнити незаповнені персональні дані, в тому числі, надавши додаткову заяву.

Стаття 17

Право на стирання («право бути забутим»)

1. Суб’єкт даних повинен мати право на стирання 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 наведених нижче 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 пунктом (a) статті 6(1) чи пунктом (a) статті 9(2), та якщо немає іншої законної підстави для опрацювання;

(c) суб’єкт даних заперечує проти опрацювання згідно зі статтею 21(1), та немає жодних першочергових законних підстав для опрацювання, або суб’єкт даних заперечує проти опрацювання згідно зі статтею 21(2);

(d) персональні дані опрацьовували незаконно;

(e) персональні дані необхідно стерти для дотримання встановленого законом 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 статті 8(1).

2. У разі, якщо контролер оприлюднив персональні дані та є зобов’язаним відповідно до параграфа 1 стерти персональні дані, контролер, з урахуванням наявних технологій та витрат на їхню реалізацію, повинен вжити відповідних заходів, у тому числі, технічних заходів, для інформування контролерів, які опрацьовують персональні дані, про те, що суб’єкт даних направив запит на стирання такими контролерами будь-яких посилань на такі персональні дані, їхні копії чи відтворення.

3. Параграфи 1 та 2 не застосовують залежно від ступеня необхідності в опрацюванні:

(a) для реалізації права на свободу вияву поглядів та свободу інформації;

(b) для дотримання встановленого законом зобов’язання, що вимагає опрацювання згідно з законодавством Союзу або держави-члена, яке поширюється на контролера, або для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера;

(c) на підставах суспільного інтересу в сфері охорони суспільного здоров’я згідно з пунктами (h) та (i) статті 9(2), а також статтею 9(3);

(d) для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей, відповідно до статті 89(1), мірою, якою вказане в параграфі 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 у разі настання 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 та суб'єкт даних виступає проти стирання персональних даних і 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 статтею 21(1) в очікуванні проведення перевірки щодо того, чи переважають законні підстави контролера над законними інтересами суб'єкта даних.

2. Якщо опрацювання було обмежено відповідно до параграфа 1, такі персональні дані необхідно, за винятком зберігання, опрацьовувати лише за згоди суб'єкта даних або для подання, реалізації або захисту правових претензій або для захисту прав іншої фізичної або юридичної особи чи на підставах важливого 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 стирання персональних даних або обмеження опрацювання

Контролер повинен повідомити про будь-яке виправлення чи стирання персональних даних або обмеження опрацювання, що здійснюють згідно зі статтею 16, статтею 17(1) і статтею 18, кожного одержувача, якому було розкрито персональні дані, за винятком, якщо 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 згідно з пунктом (a) статті 6(1) чи пунктом (a) статті 9(2), або на основі договору згідно з пунктом (b) статті 6(1); та

(b) опрацювання є автоматизованим.

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

3. Реалізація права, вказаного в параграфі 1 цієї статті, не повинна обмежувати дію статті 17. Це право не застосовується до опрацювання, необхідного для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера.

4. Право, вказане в параграфі 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 пункту (e) чи (f) статті 6(1), у тому числі, проти профайлінгу, що ґрунтується на тих положеннях. Контролер не повинен більше опрацьовувати персональні дані за винятком доведення ним наявності 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, право, вказане в параграфах 1 і 2, необхідно чітко довести до відома суб'єкта даних і представити 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 статистичних цілей згідно зі статтею 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 є необхідним для виконання завдання на підставах суспільного інтересу.

Стаття 22

Автоматизоване індивідуальне вироблення й ухвалення рішень, у тому числі, профайлінг

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

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 пунктах (a) та (c) параграфа 2, контролер даних повинен вжити належних заходів для гарантування охорони прав, свобод, законних інтересів суб'єктів даних, принаймні права на людське втручання з боку контролера, висловлення своєї думки та оскарження рішення.

4. Рішення, вказані в параграфі 2, не повинні ґрунтуватися на спеціальних категоріях персональних даних, вказаних у статті 9(1), за винятком застосування пункту (a) або (g) статті 9(2) та відсутності передбачених належних заходів щодо 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 інструменту обсяг обов'язків і прав, передбачений в статтях 12–22 і статті 34, а також статті 5, відповідно до того, наскільки його положення відображають права і обов'язки, передбачені в статтях 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 або запобіганню загрозам громадській безпеці;

(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 суспільного 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 пунктах (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) обсяг введених 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 категорій опрацювання;

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

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

ГЛАВА 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 їхньої 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 статті 40, чи затверджених механізмів сертифікації, як вказано в статті 42, можна використовувати як елемент 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 власне 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 замовчуванням опрацьовують лише ті персональні дані, які є необхідними для кожної спеціальної цілі опрацювання. Такий обов'язок застосовують до кількості зібраних персональних даних, ступеня їхнього опрацювання, періоду їхнього зберігання та їхньої доступності. Зокрема, такими заходами необхідно гарантувати ненадання за замовчуванням доступу до персональних даних без звернення особи до невизначеної кількості фізичних осіб.

3. Затверджений механізм сертифікації, відповідно до статті 42, можна використовувати як елемент підтвердження відповідності вимогам, встановленим у параграфах 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 встановити свої відповідні обов'язки, що відображають зміст зобов'язань за цим Регламентом, зокрема, щодо реалізації

прав суб'єкта даних і їхніх відповідних обов'язків щодо надання інформації, вказаної в статтях 13 і 14, шляхом досягнення домовленості між ними, за винятком, якщо, та оскільки, відповідні обов'язки контролерів не визначено законодавством Союзу або держави-члена, дія якого поширюється на контролерів. За домовленістю можна призначити координаційний центр для суб'єктів даних.

2. Домовленість, вказана в параграфі 1, повинна належним чином відображати відповідні ролі та відносини спільних контролерів щодо суб'єктів даних. Сутність домовленості необхідно повідомити суб'єкту даних.

3. Незалежно від умов домовленості, вказаних у параграфі 1, суб'єкт даних може скористатися своїми правами за цим Регламентом щодо та проти кожного з контролерів.

Стаття 27

Представники контролерів або операторів, які не мають осідків у Союзі

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

2. Обов'язок, установлений у параграфі 1 цієї статті, не застосовують до:

(a) опрацювання, яке призначено для окремого випадку, воно не передбачає, у великих обсягах, опрацювання спеціальних категорій даних, як вказано в статті 9(1), або опрацювання даних про судимості і кримінальні злочини, вказані в статті 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 або оператора, зокрема, наглядові органи і суб'єкти даних, з усіх питань, пов'язаних з опрацюванням, з метою забезпечення відповідності цьому Регламенту.

5. Призначення представника контролером або оператором необхідно здійснювати 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 таких 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 без отримання попереднього спеціального чи загального письмового дозволу контролера. У випадку загального письмового дозволу, оператор повинен повідомити контролера про будь-які цілеспрямовані зміни щодо 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 та встановлює предмет і тривалість опрацювання, специфіку і 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 існування відповідної вимоги законодавством Союзу або держави-члена, яка поширюється на оператора; у такому випадку, оператор інформує контролера про таку законодавчу вимогу до початку опрацювання, за винятком, якщо таким законодавством заборонено надання такої інформації на важливих підставах суспільного інтересу;

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

(c) вживає усіх заходів, необхідних відповідно до статті 32;

(d) дотримується умов, вказаних у параграфах 2 і 4 щодо залучення додаткового оператора;

(e) враховуючи специфіку опрацювання, допомагає контролеру належними технічними та організаційними заходами, наскільки це можливо, для виконання обов'язку контролера відповідати на запити щодо реалізації прав суб'єкта даних, установлених у главі III;

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

(g) на розсуд контролера, видаляє або повертає усі персональні дані контролеру після постачання послуг, пов'язаних з опрацюванням, і видаляє наявні копії, за винятком існування у законодавстві Союзу або держави-члена вимоги 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 або інший аудитор відповідно до мандату, наданого контролером.

З урахування пункту (h) першого підпараграфа, оператор негайно інформує контролера, якщо, на його думку, вказівка порушує цей Регламент або інші положення законодавства Союзу або держави-члена щодо захисту даних.

4. У разі залучення оператором додаткового оператора до здійснення спеціального опрацювання даних від імені контролера, ті самі обов'язки щодо захисту даних, які встановлено між контролером або оператором в договорі або іншому нормативно-правовому акті, як вказано в параграфі 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 таким, що повністю відповідає перед контролером за виконання обов'язків такого додаткового оператора.

5. Дотримання оператором затвердженого кодексу поведінки, як вказано в статті 40, чи затвердженого механізму сертифікації, як вказано в статті 42, можна використовувати як елемент підтвердження достатніх гарантій, як вказано в параграфах 1 та 4 цієї статті.

6. Без обмеження окремого договору між контролером і оператором, договір або інший нормативно-правовий акт, вказані в параграфах 3 і 4 цієї статті, може ґрунтуватися, в цілому чи частково, на стандартних договірних положеннях, вказаних у параграфах 7 і 8 цієї статті, в тому числі, якщо вони є частиною сертифікації, наданої контролеру або оператору відповідно до статей 42 і 43.

7. Комісія може встановлювати стандартні договірні положення з питань, вказаних у параграфах 3 і 4 цієї статті, та відповідно до експертної процедури, вказаної в статті 93(2).

8. Наглядовий орган може ухвалити стандартні договірні положення з питань, вказаних у параграфах 3 і 4 цієї статті, та відповідно до механізму послідовності, вказаного в статті 63.

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

10. З дотриманням положень статей 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 або оператора, що має доступ до персональних даних, не повинні опрацьовувати такі дані без інструкцій контролера, за винятком відповідної вимоги законодавства Союзу або держави-члена.

Стаття 30

Записи опрацювання даних

1. Кожний контролер і, за необхідності, представник контролера повинні вести запис 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) опис категорій суб’єктів даних і категорій персональних даних;

(d) категорії одержувачів, яким персональні дані були або будуть розкриті, в тому числі одержувачі в 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, вказаних у другому підпараграфі статті 49(1), документацію відповідних гарантій;

(f) за можливості, — передбачені часові обмеження для стирання різних категорій даних;

(g) за можливості, — загальний опис технічних і організаційних заходів безпеки, вказаних у статті 32(1).

2. Кожний оператор і, за необхідності, представник оператора повинні вести запис усіх категорій опрацювання, які здійснюють від імені контролера, що містить інформацію про:

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

(b) категорії опрацювання, що 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, вказаних у другому підпараграфі статті 49(1), документацію відповідних гарантій;

(d) за можливості, — загальний опис технічних і організаційних заходів безпеки, вказаних у статті 32(1).

3. Записи, вказані в параграфах 1 і 2, повинні бути оформлені в письмовій формі, в тому числі, — в електронній.

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

5. Обов'язки, вказані в параграфах 1 і 2, не можна застосовувати до підприємства чи організації з кількістю працівників, меншою за 250 осіб, за винятком, якщо 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 статті 9(1), або персональні дані про судимості і кримінальні злочини, вказані в статті 10.

Стаття 31

Співпраця із наглядовим органом

Контролер і оператор та, за необхідності, їхні представники, повинні співпрацювати, на запит, з наглядовим органом у виконанні своїх завдань.

Секція 2

Безпека персональних даних

Стаття 32

Безпека опрацювання

1. Зважаючи на 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, між іншим, у належних випадках:

(a) використання псевдонімів і шифрування персональних даних;

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

(c) здатність вчасно відновити наявність і доступ до персональних даних у випадку технічної аварії;

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

2. Оцінюючи належний 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 вказано в статті 40, чи затверджених механізмів сертифікації, як вказано в статті 42, можна використовувати як елемент підтвердження відповідності вимогам, встановленим у параграфі 1 цієї статті.

4. Контролер і оператор повинні вжити заходів для того, щоб забезпечити, що будь-яка фізична особа, яка діє під керівництвом контролера або оператора і має доступ до персональних даних, не опрацьовує їх, за винятком, якщо вона здійснює це за інструкціями контролера, окрім випадків, 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 випадку порушення захисту персональних даних, контролер повинен без необґрунтованої затримки та, за можливості, не пізніше, ніж протягом 72 години після того, як йому стало відомо про це, повідомити про порушення захисту персональних даних наглядовий орган, який є компетентним згідно зі статтею 55, якщо таке порушення навряд чи призведе до виникнення ризику для прав і свобод фізичних осіб. Якщо нотифікацію наглядового органу не здійснюють 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. Нотифікація, вказана в параграфі 1, повинна принаймні:

(a) описувати 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) повідомляти особу та контактні дані співробітника з питань захисту даних або іншого координаційного органу, де можна отримати більше інформації;

(c) описувати ймовірні наслідки порушення захисту персональних даних;

(d) описувати заходи, яких було вжито чи яких запропоновано вжити контролером для реагування на порушення захисту персональних даних, у тому числі, в разі необхідності, заходи для зниження його потенційних негативних наслідків.

4. Якщо і оскільки є неможливим надати інформацію одночасно, інформацію можна надавати поетапно без подальшої необґрунтованої затримки.

5. Контролер повинен зафіксувати будь-які порушення захисту персональних даних, збираючи факти, що стосуються порушення захисту персональних даних, його наслідків та вжитих заходів щодо виправлення ситуації. Документація надає можливість наглядовому органу перевірити відповідність цій статті.

Стаття 34

Повідомлення суб'єкта даних про порушення захисту персональних даних

1. Якщо порушення захисту персональних даних ймовірно призведе до виникнення високого ризику 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, вказане в параграфі 1 цієї статті, описує, з використанням чітких і простих формулювань, специфіку порушення захисту персональних даних і містить принаймні інформацію та заходи, вказані в пунктах (b), (c) і (d) статті 33(3).

3. Повідомлення суб'єкта даних, вказане в параграфі 1, є необов'язковим у разі виконання однієї з наведених нижче вимог:

(a) контролер вжив необхідних технічних та організаційних заходів захисту, і такі заходи було 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 наступних заходів, що гарантують, що високий ризик для прав і свобод суб'єктів даних, вказаний у параграфі 1, ймовірно більше не матеріалізується;

(c) воно передбачатиме докладання надмірних зусиль. У такому разі замість нього надають публічне повідомлення чи подібний інструмент, за допомогою якого повідомляють суб'єктів даних у рівноцінно дієвий спосіб.

4. Якщо контролер ще не повідомив суб'єкта даних про порушення захисту персональних даних, наглядовий орган, розглянувши ймовірність спричинення порушенням захисту

персональних даних високого ризику, може вимагати зробити це чи може вирішити, що будь-яку з умов, вказаних в параграфі 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, до здійснення опрацювання, повинен провести оцінювання впливу передбачених операцій опрацювання на захист персональних даних. Єдине оцінювання може стосуватися низки подібних операцій опрацювання, що становлять подібні високі ризики.

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

3. Оцінювання впливу на захист даних, вказане в параграфі 1, є необхідним, зокрема, у випадку:

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

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

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

4. Наглядовий орган повинен розробити і оприлюднити перелік операцій опрацювання, на які поширюється вимога проведення оцінювання впливу на захист даних відповідно до параграфа 1. Наглядовий орган повідомляє Раду про такі переліки, як вказано в статті 68.

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

6. До ухвалення переліків, вказаних у параграфах 4 і 5, компетентний наглядовий орган повинен застосовувати механізм послідовності, вказаний у статті 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 вільний рух персональних даних у межах Союзу.

7. Оцінювання повинне містити принаймні:

(a) систематичний опис передбачених операцій опрацювання та цілі опрацювання, в тому числі, за необхідності, законний інтерес контролера;

(b) оцінювання необхідності та пропорційності операцій опрацювання щодо цілей;

(c) оцінювання ризиків для прав і свобод суб’єктів даних, вказаних у параграфі 1; та

(d) заходи, передбачені для боротьби з ризиками, в тому числі, гарантії, заходи безпеки та механізми забезпечення захисту персональних даних та 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 статті 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 щодо запланованого опрацювання, без обмеження захисту комерційних або суспільних інтересів або безпеки операцій опрацювання.

10. Якщо опрацювання відповідно пункту (c) або (e) статті 6(1) має законодавчу базу відповідно до законодавства Союзу або законодавства 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 проведено як частину загального оцінювання впливу в контексті ухвалення такої законодавчої бази, параграфи 1–7 не застосовують, за винятком, якщо держави-члени вважають за необхідне провести таке оцінювання до здійснення опрацювання даних.

11. У разі необхідності, контролер повинен провести перевірку, щоб пересвідчитися, чи здійснюють опрацювання з урахуванням 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 до початку здійснення опрацювання, якщо оцінка впливу на захист даних за статтею 35 свідчить про те, що опрацювання призведе до виникнення високого ризику в разі відсутності заходів, які вживає контролер для зниження ризику.

2. Якщо наглядовий орган вважає, що заплановане опрацювання, вказане в параграфі 1, може порушити цей Регламент, зокрема, якщо контролер недостатньо ідентифікував або знизив ризик, наглядовий орган, протягом періоду до 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 статті 58. Цей період може бути подовжено на шість тижнів, з огляду 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 такої затримки. Такі періоди може бути призупинено до отримання наглядовим органом інформації, яку він запитував для цілей консультації.

3. Надаючи консультацію наглядовому органу відповідно до параграфа 1, контролер повинен надати наглядовому органу:

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

(b) цілі та засоби запланованого опрацювання;

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

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

(e) оцінку впливу на захист даних, передбачену в статті 35; і

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

4. Держави-члени повинні надати наглядовому органу консультацію під час підготування пропозиції для законодавчого інструменту, який повинен ухвалити національний парламент, або регуляторного інструменту на підставі такого законодавчого інструменту, що стосується опрацювання.

5. Без обмеження положень параграфа 1, законодавство держав-членів може вимагати від контролерів проводити консультації та отримувати попередній дозвіл від наглядового органу щодо опрацювання контролером для реалізації завдання, яке виконує контролер для цілей 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 наведених нижче випадків:

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

(b) основні види діяльності контролера або оператора становлять операції опрацювання, які, в силу їхньої специфіки, обсягів та/чи цілей, вимагають регулярного, систематичного і широкомасштабного моніторингу суб'єктів даних; або

(c) основні види діяльності контролера або оператора становлять широкомасштабне опрацювання спеціальних категорій даних відповідно до статті 9 та персональних даних про судимості і кримінальні злочині, вказані в статті 10.

2. Група підприємств може призначити єдиного співробітника з питань захисту даних за умови, що в кожному осідку існує доступ до співробітника з питань захисту даних.

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

4. У ситуаціях, відмінних від тих, що вказано в параграфі 1, контролер або оператор чи асоціації та інші органи, що представляють категорії контролерів або операторів можуть або, відповідно до вимог законодавства Союзу або 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 на підставі професійних якостей і, зокрема, експертних знань із права та практики захисту даних, а також здатності виконувати завдання, вказані в статті 39.

6. Співробітник з питань захисту даних може бути членом персоналу 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, вказаних у статті 39, шляхом надання ресурсів, необхідних для реалізації таких завдань і доступу до персональних даних, операцій опрацювання, та для 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 виконання їхніх завдань. Співробітник з питань захисту даних безпосередньо звітує до найвищого управлінського рівня 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 і обов'язки. Контролер або оператор забезпечують, щоб жодні такі завдання та обов'язки не призвели до 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, 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 моніторинг його проведення відповідно до статті 35;

(d) співпрацювати із наглядовим органом;

(e) діяти як координаційний центр для наглядового органу з питань, що стосуються опрацювання, в тому числі, попередньої консультації, вказаної в статті 36, і надавати консультації за необхідності, щодо будь-якого іншого питання.

2. Під час виконання своїх завдань співробітник з питань захисту даних повинен належним чином враховувати ризик, пов'язаний із операціями опрацювання, зважаючи на 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, беручи до уваги особливі характеристики різних секторів опрацювання та конкретні потреби 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, або розширити такі 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, та їхнього захисту, і способу, яким необхідно отримувати згоду носіїв батьківської відповідальності щодо дітей;

(h) заходів і процедур, вказаних у статтях 24 і 25, і заходів для гарантування безпеки опрацювання, вказаних у статті 32;

(i) нотифікації наглядових органів про порушення захисту персональних даних та повідомлення суб'єктів даних про такі порушення захисту персональних даних;

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

(k) позасудових процедур і 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 статей 77 і 79.

3. Окрім дотримання контролерами або операторами відповідно до цього Регламенту, кодекси поведінки, що затверджені відповідно до параграфа 5 цієї статті та мають загальну дію відповідно до параграфа 9 цієї статті, також можна застосовувати до контролерів або операторів, на яких не поширюється дія цього Регламенту відповідно до статті 3 для того, щоб надати належні гарантії в межах передавання персональних даних до третіх країн чи міжнародних організацій на умовах, наведених у пункті (e) статті 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.

4. Кодекс поведінки, вказаний у параграфі 2 цієї статті, повинен передбачати механізми, що дозволяють органу, вказаному в статті 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 статті 55 або 56.

5. Асоціації та інші органи, вказані в параграфі 2 цієї статті, що мають намір підготувати кодекс поведінки чи внести зміни та доповнення або розширити наявний кодекс, подають проект кодексу, змін та доповнень або розширення до наглядового органу, що є компетентним відповідно до статті 55. Наглядовий орган надає висновок про те, чи відповідає проект кодексу, змін та доповнень або розширення цьому Регламенту, та затверджує такий проект кодексу, змін та доповнень або розширення, якщо з'ясовує, що в ньому передбачено достатні належні гарантії.

6. Якщо проект кодексу, змін та доповнень або розширення затверджують відповідно до параграфа 5, та якщо відповідний кодекс поведінки не стосується опрацювання даних в декількох державах-членах, наглядовий орган реєструє і опубліковує кодекс.

7. Якщо проект кодексу стосується опрацювання даних в декількох державах-членах, наглядовий орган, що є компетентним відповідно до статті 55, до затвердження проекту кодексу, змін та доповнень або розширення, подає його на процедуру, вказану в статті 63, до Ради, яка надає висновок щодо того, чи відповідає проект кодексу, змін та доповнень або розширення цьому Регламенту або, в ситуації, вказаній в параграфі 3 цієї статті, чи передбачено в ньому належні гарантії.

8. Якщо висновок, вказаний у параграфі 7, підтверджує, що проект кодексу, змін та доповнення або розширення відповідає цьому Регламенту або, в ситуації, вказаній в параграфі 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 та доповнень або розширення, що подають їй відповідно до параграфа 8 цієї статті, мають загальну дію в межах Союзу. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, встановленої в статті 93(2).

10. Комісія забезпечує належну публічність для затверджених кодексів, щодо яких було прийнято рішення про те, що вони мають загальну дію згідно з параграфом 9.

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

Стаття 41

Моніторинг затверджених кодексів поведінки

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

2. Орган, як вказано в параграфі 1, може бути акредитований для моніторингу дотримання кодексу поведінки, якщо такий орган:

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

(b) запровадив процедури, що дозволяють йому проводити 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 було 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 призводять до конфлікту інтересів.

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

4. Без порушення завдань і повноважень компетентного наглядового органу та положень глави VIII, орган, як вказано в параграфі 1 цієї статті, з урахуванням належних гарантій, вживає необхідних дій у випадках порушення кодексу контролером або оператором, у тому числі призупинення роботи чи виключення залученого контролера або оператора з кодексу. Він повідомляє компетентний наглядовий орган про такі дії та причини їх вжиття.

5. Компетентний наглядовий орган відкликає акредитацію органу, як вказано в параграфі 1, якщо умови для акредитації не виконано чи більше не виконують, або якщо дії, яких вживає орган, порушують цей Регламент.

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 та штампів і знаків захисту даних з

метою підтвердження відповідності цьому Регламенту операцій опрацювання, які здійснюють контролери і оператори. Необхідно брати до уваги особливі потреби мікропідприємств, малих і середніх підприємств.

2. Окрім дотримання контролерами або операторами відповідно до цього Регламенту, механізми сертифікації захисту даних, штампи і знаки, затверджені відповідно до параграфа 5 цієї статті, можна запровадити з метою підтвердження наявності належних гарантій, які надають контролери або оператори, на яких не поширюється дія цього Регламенту відповідно до статті 3 в межах передавання персональних даних до третіх країн чи міжнародних організацій на умовах, вказаних у пункті (f) статті 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 ступінь відповідальності контролера або оператора щодо відповідності цьому Регламенту та не обмежує завдання і повноваження наглядових органів, що є компетентними відповідно до статті 55 чи 56.

5. Сертифікацію відповідно до цієї статті видають органи сертифікації, вказані в статті 43, або компетентні наглядові органи, на підставі критеріїв, затверджених таким компетентним наглядовим органом згідно зі статтею 58(3) або Радою згідно зі статтею 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 статті 43, або, у разі необхідності, компетентному наглядовому органу, всю інформацію та доступ до опрацювання даних, що є необхідним для проведення процедури сертифікації.

7. Сертифікацію видають контролеру або оператору на строк до трьох років, її може бути поновлено на тих самих умовах, якщо і надалі буде виконано відповідні вимоги. Сертифікацію відкликають, у разі необхідності, органи сертифікації, вказані в статті 43, або компетентний наглядовий орган, якщо вимоги для сертифікації не виконано або більше не виконують.

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

Стаття 43

Органи сертифікації

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

(a) наглядовим органом, що є компетентним згідно зі статтею 55 чи 56;

(b) національним органом з акредитації, названим відповідно до Регламенту Європейського Парламенту і Ради (ЄС) № 765/2008 ([1]) згідно з EN-ISO/IEC 17065/2012 та додатковими вимогами, встановленими наглядовим органом, що є компетентним згідно зі статтею 55 чи 56.

([1]) Регламент Європейського Парламенту і Ради (ЄС) № 765/2008 від 9 липня 2008 року про вимоги до акредитації та ринкового нагляду стосовно реалізації продуктів, та про скасування Регламенту (ЄЕС) № 339/93 (OB L 218, 13.08.2008, с. 30).

2. Органи сертифікації, вказані в параграфі 1, необхідно акредитувати згідно з цим параграфом, лише якщо вони:

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

(b) зобов'язались поважати критерії, вказані в статті 42(5) і затверджені наглядовим органом, що є компетентним згідно зі статтею 55 чи 56 або Радою відповідно до статті 63;

(c) розробили процедури для видачі, періодичної перевірки та відкликання сертифікації 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 призводять до конфлікту інтересів.

3. Акредитацію органів сертифікації, як вказано в параграфах 1 і 2 цієї статті, здійснюють на підставі критеріїв, затверджених наглядовим органом, що є компетентним згідно зі статтею 55 чи 56 або Радою відповідно до статті 63. У випадку акредитації відповідно до пункту (b) параграфа 1 цієї статті, ці вимоги доповнюють ті, що передбачені в Регламенті (ЄС) № 765/2008, і технічні норми, що описують методи та процедури органів сертифікації.

4. Органи сертифікації, вказані в параграфі 1, несуть відповідальність за належне оцінювання, в результаті якого можна видати або відкликати сертифікацію без обмеження відповідальності контролера або оператора за дотримання цього Регламенту. Акредитацію видають на строк до п'яти років, її можна поновлювати на тих самих умовах, якщо орган сертифікації відповідає вимогам, встановленим в цій статті.

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

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

7. Дотримуючись положень глави VIII, компетентний наглядовий орган або національний орган з акредитації анулює акредитацію органу сертифікації відповідно до параграфа 1 цієї статті, якщо умови для акредитації виконано або їх більше не виконують, або якщо дії, яких вживає орган сертифікації, порушують положення цього Регламенту.

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

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

ГЛАВА V

Передавання персональних даних до третіх країн або міжнародних організацій

Стаття 44

Загальні принципи передавання

Будь-яке передавання персональних даних, що перебувають в процесі опрацювання чи призначені для опрацювання після передавання до третьої країни чи міжнародної організації, повинне відбуватися лише у разі, якщо з урахуванням інших положень цього Регламенту контролер і оператор дотримуються умов, встановлених в цій главі, 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 відсутності порушення рівня 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, забезпечує належний рівень захисту. Таке передавання не вимагає отримання будь-якого спеціального дозволу.

2. Під час оцінювання відповідності рівня 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 для 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, що 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, після проведення оцінювання адекватності рівня захисту, може вирішити, у формі імплементаційного акту, що третя країна, територія чи один або декілька визначених секторів у межах третьої країни, або міжнародна організація забезпечує належний рівень захисту даних у значенні параграфа 2 цієї статті. Імплементаційний акт передбачає механізм періодичного перегляду, щонайменше кожні чотири роки, який повинен враховувати усі належні тенденції розвитку в третій країні чи міжнародній організації. Імплементаційний акт уточнює територіальне та секторальне застосування та, за необхідності, визначає наглядовий орган або органи, вказані в пункті (b) параграфа 2 цієї статті. Імплементаційний акт ухвалюють відповідно до експертної процедури, вказаної в статті 93(2).

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

5. Комісія, якщо наявна інформація відображає, зокрема після перегляду, як вказано в параграфі 3 цієї статті, що третя країна, територія чи один або декілька визначених секторів в межах третьої країни, чи міжнародна організація більше не забезпечує належний рівень

захисту в значенні параграфа 2 цієї статті, необхідною мірою, скасовує, вносить зміни та доповнення, або призупиняє рішення, вказане в параграфі 3 цієї статті за шляхом ухвалення імплементаційних актів, що не мають зворотної сили. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, вказаної в статті 93(2).

Зважаючи на належним чином підтверджену термінову необхідність, Комісія повинна негайно ухвалити застосовні імплементаційні акти у порядку, як це вказано в статті 93(3).

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

7. Рішення відповідно до параграфа 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 статтями 46–49.

8. Комісія опубліковує 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 більше не забезпечується належний рівень захисту.

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

Стаття 46

Передавання з урахуванням належних гарантій

1. За відсутності рішення відповідно до статті 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 умови наявності прав суб'єктів даних, що підлягають забезпеченню їхньої реалізації, та дієвих засобів правового захисту для суб'єктів даних.

2. Належні гарантії, вказані в параграфі 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 статтею 47;

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

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

(e) затвердженим кодексом поведінки відповідно до статті 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 статті 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 параграфі 1, можна також надавати, зокрема:

(a) положеннями договору між контролером або оператором та 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 статті 63 у випадках, вказаних у параграфі 3 цієї статті.

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

Стаття 47

Зобов'язальні корпоративні правила

1. Компетентний наглядовий орган затверджує зобов'язальні корпоративні правила відповідно до механізму послідовності, встановленого в статті 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 здійснюють спільну господарську діяльність, в тому числі, їхні працівники;

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

(c) відповідають вимогам, встановленим у параграфі 2.

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

(a) структуру та контактні дані групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, та кожного з їхніх 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) їхню 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, права не підлягати рішенням, що ґрунтуються виняткова на автоматизованому опрацюванні, в тому числі, профайлінгу відповідно до статті 22, права подавати скаргу до компетентного наглядового органу та компетентних судів держав-членів згідно зі статтею 79, та отримувати 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 за умов доведення, 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 пунктах (d), (e) і (f) цього параграфа, надають суб'єктам даних, в доповнення до статей 13 і 14;

(h) завдання будь-якого співробітника з питань захисту даних, призначеного відповідно до статті 37, або будь-якої іншої особи чи установи, відповідальної за моніторинг дотримання зобов'язальних корпоративних правил в межах групи підприємств або групи підприємств, що здійснюють 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 здійснюють спільну господарську діяльність, для забезпечення перевірки відповідності зобов'язальним корпоративним правилам. Такі механізми передбачають перевірки захисту даних і методи забезпечення вжиття виправних дій для захисту прав суб'єкта даних. Результати такої перевірки необхідно повідомляти особі чи установі, вказаній в пункті (h), і раді контролюючого підприємства групи підприємств чи групи підприємств, що здійснюють спільну господарську діяльність, та надавати на запит компетентного наглядового органу;

(k) механізми для звітування та запису 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 здійснюють спільну господарську діяльність, зокрема шляхом надання наглядовому органу результатів перевірок заходів, вказаних у пункті (j);

(m) механізми для звітування до компетентного наглядового органу про будь-які законні вимоги, які поширюються на члена групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність в 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 для 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 статті 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, і Союзом або державою-членом, без обмеження інших підстав для передавання відповідно до цієї глави.

Стаття 49

Відступи для спеціальних ситуацій

1. За відсутності рішення про відповідність згідно зі статтею 45(3) або належних гарантій відповідно до статті 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 та 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 на важливих підставах 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, встановлені законодавством Союзу або держави-члена.

Якщо передавання не можна обґрунтувати на підставі положення статті 45 чи 46, в тому числі положень про зобов’язальні корпоративні правила, та жодний з відступів, застосовних до спеціальної ситуації, вказаної в першому підпараграфі цього параграфа, не є застосовним, передавання до третьої країни чи до міжнародної організації може мати місце лише у разі, якщо передавання не є повторюваним, стосується лише обмеженої кількості суб’єктів даних, є необхідним для цілей 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 статтях 13 і 14, контролер інформує суб’єкта даних про передавання та свої істотні законні інтереси, що їх він переслідує.

2. Передавання відповідно до пункту (g) першого підпараграфа параграфа 1 не включає 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) першого підпараграфа параграфа 1 та його другого підпараграфа не застосовують до видів діяльності, які здійснюють органи публічної влади під час виконання своїх публічних повноважень.

4. Суспільний інтерес, вказаний в пункті (d) першого підпараграфа параграфа 1, визнається в законодавстві Союзу чи законодавстві 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 другому підпараграфі параграфа 1 цієї статті, у формі записів, вказаних у статті 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 для 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 нотифікацію, звернення скарг, допомогу в проведенні розслідувань та обмін інформацією, з урахуванням необхідних гарантій для захисту персональних даних і інших фундаментальних прав і свобод;

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

(d) сприяння обміну та документації законодавства і практики захисту персональних даних, у тому числі щодо юрисдикційних колізій з третіми країнами.

ГЛАВА 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 руху 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 засновують більше, аніж один наглядовий орган, така держава-член призначає наглядовий орган, що повинен представляти такі органи в Раді, та встановлює механізм забезпечення дотримання іншими органами правил щодо механізму послідовності, вказаного в статті 63.

4. Кожна держава-член повідомляє Комісію про положення свого закону, який вона ухвалює відповідно до цієї глави, до 25 травня 2018 року 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 та здійснення своїх повноважень згідно з цим Регламентом.

2. Член або члени кожного наглядового органу, під час виконання своїх завдань та 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-якої дії, що є несумісною з їхніми обов’язками, та не повинні, протягом строку їхніх повноважень, займатися будь-якою несумісною діяльністю, прибутковою чи ні.

4. Кожна держава-член забезпечує, щоб кожний наглядовий орган мав у своєму розпорядженні людські, технічні та фінансові ресурси, приміщення та інфраструктуру, необхідну для результативного виконання своїх завдань та здійснення своїх повноважень, у тому числі тих, які здійснюють в контексті взаємної допомоги, співпраці та участі в Раді.

5. Кожна держава-член забезпечує, щоб кожен наглядовий орган обирав і мав свій власний персонал, що підпорядковується безпосередньому керівництву відповідного члена чи членів наглядового органу.

6. Кожна держава-член забезпечує, щоб кожний наглядовий орган підлягав фінансовому контролю, що не впливає на його незалежність, і мав окремі, публічні річні бюджети, що може бути частиною загальнодержавного або національного бюджету.

Стаття 53

Загальні умови для членів наглядового органу

1. Держави-члени забезпечують, щоб кожного члена їхніх наглядових органів було призначено у порядку прозорої процедури:

— їхній парламент;

— їхній уряд;

— їхній голова держави; або

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

2. Кожний член повинен мати кваліфікації, досвід і вміння, зокрема, в сфері захисту персональних даних, які є необхідними для виконання його обов'язків та 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 у випадках серйозного проступку абр якщо член більше не дотримується умов, необхідних для виконання обов'язків.

Стаття 54

Правила заснування наглядового органу

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

(a) заснування кожного наглядового органу;

(b) кваліфікації та умови прийнятності, необхідні для призначення як члена кожного наглядового органу;

(c) правила і процедури для призначення члена чи членів кожного наглядового органу;

(d) тривалість строку повноважень члена чи членів кожного наглядового органу становить не менше чотирьох років, за винятком першого призначення після 24 травня 2016 року, 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 кожного наглядового органу;

(f) умови, що регулюють обов'язки члена чи членів і персоналу кожного 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 та персонал кожного наглядового органу поширюється, згідно з законодавством Союзу або держави-члена, обов'язок збереження професійної таємниці як

протягом, так і після строку їхніх повноважень, щодо будь-якої конфіденційної інформації, про яку вони дізналися під час виконання своїх завдань або реалізації своїх повноважень. Під час строку їхніх повноважень, такий обов'язок збереження професійної таємниці, зокрема, застосовують до звітування 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 здійснюється публічними органами або приватними органами, які діють на підставі пункту (c) або (e) статті 6(1), компетенцію має наглядовий орган відповідної держави-члена. У таких випадках статтю 56 не застосовують.

3. Наглядові органи не мають компетенції здійснювати нагляд за операціями опрацювання, які здійснюють суди, діючи як судові інстанції.

Стаття 56

Компетенція керівного наглядового органу

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

2. Відступаючи від параграфа 1, кожний 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, вказаних у параграфі 2 цієї статті, наглядовий орган повідомляє керівний наглядовий орган без затримки про таке питання. Протягом тритижневого періоду з дати отримання повідомлення керівний наглядовий орган повинен вирішити, чи розглядатиме справу згідно з процедурою, передбаченою в статті 60, зважаючи на те, чи знаходиться осідок контролера або оператора в державі-члені, з якої наглядовий орган повідомив про це.

4. Якщо керівний наглядовий орган вирішує розглядати справу, застосовують процедуру, передбачену в статті 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 статті 60(3).

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

6. Керівний наглядовий орган є єдиним посередником контролера або оператора в транскордонному опрацюванні, яке здійснює такий контролер або оператор.

Стаття 57

Завдання

1. Без обмеження інших завдань, встановлених згідно з цим Регламентом, кожний 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. Особливу увагу необхідно приділити опрацюванню, спрямованому безпосередньо на дітей;

(c) консультує, згідно з законодавством держави-члена, національний парламент, уряд і інші установи та органи щодо законодавчих і адміністративних інструментів, що пов'язані з захистом прав і свобод фізичних осіб у зв'язку з опрацюванням;

(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 їхніх 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 статтею 80, і розслідує, наскільки це можливо, предмет скарги та повідомляє позивача про прогрес 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 забезпечення виконання цього Регламенту;

(h) проводить 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, вказані в статті 28(8) та пункті (d) статті 46(2);

(k) започатковує і веде список у зв'язку з вимогами для оцінювання впливу на захист даних згідно зі статтею 35(4);

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

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

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

(o) за необхідності, здійснює періодичний перегляд сертифікацій, виданих згідно зі статтею 42(7);

(p) розробляє і опубліковує критерії для акредитації органу для моніторингу кодексів поведінки згідно зі статтею 41 чи органу сертифікації згідно зі статтею 43;

(q) проводить акредитацію органу для моніторингу кодексів поведінки згідно зі статтею 41 чи органу сертифікації згідно зі статтею 43;

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

(s) ухвалює зобов'язальні корпоративні правила відповідно до статті 47;

(t) сприяє діяльності Ради;

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

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

2. Кожний наглядовий орган полегшує подання скарг, вказаних у пункті (f) параграфа 1 за допомогою заходів, таких як форма подання скарги, яку також можна оформити в електронному форматі без обмеження інших засобів зв'язку.

3. Виконання завдань кожного наглядового органу здійснюють 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 їхнє багаторазове повторення, наглядовий орган може стягувати розумну плату, що ґрунтується на адміністративних витратах, або ухилитися від виконання дій на запит. Наглядовий орган повинен нести тягар доведення явно необґрунтованого чи надмірного характеру запиту.

Стаття 58

Повноваження

1. Кожний 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, яку він вимагає для виконання своїх завдань;

(b) проводити розслідування в формі перевірок захисту даних;

(c) здійснювати перегляд сертифікацій, виданих згідно зі статтею 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. Кожний наглядовий орган має всі виправні повноваження, а саме:

(a) надсилати попередження контролеру або оператору про те, що призначені операції опрацювання ймовірно порушать положення 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 привести операції опрацювання у відповідність 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 здійснити виправлення чи стирання персональних даних або обмеження опрацювання згідно зі статтями 16, 17 і 18, і нотифікацію про такі дії кожного одержувача, якому було розкрито персональні дані відповідно до статті 17(2) і статті 19;

(h) відкликати сертифікацію чи наказати органу сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43, або наказати органу сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються;

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

(j) наказувати призупинення потоків даних до одержувача в третій країні чи до міжнародної організації.

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

(a) консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36;

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

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

(d) надавати висновок і затверджувати проекти кодексів поведінки відповідно до статті 40(5);

(e) надавати акредитацію органам сертифікації відповідно до статті 43;

(f) видавати сертифікації та затверджувати критерії сертифікації відповідно до статті 42(5);

(g) ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2);

(h) надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3);

(i) надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3);

(j) затверджувати зобов'язальні корпоративні правила відповідно до статті 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 в законодавстві Союзу або держави-члена згідно з Хартією.

5. Кожна держава-член забезпечує на законодавчому рівні, щоб її наглядовий орган було наділено повноваженням виносити порушення цього Регламенту до уваги судових органів 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 вказано в параграфах 1, 2 і 3. Реалізація таких повноважень не повинна перешкоджати результативному застосуванню глави VII.

Стаття 59

Звіти про виконану роботу

Кожний наглядовий орган складає щорічний звіт про свою діяльність, що може містити список типів порушення, про які було повідомлено, та типи заходів, яких було вжито відповідно до статті 58(2). Ці звіти передають до національного парламенту, уряду та інших органів, як це призначено законодавством держави-члена. Громадськість, Комісія та Рада отримують до них доступ.

ГЛАВА VII

Співпраця і послідовність

Секція 1

Співпраця

Стаття 60

Співпраця між керівним наглядовим органом і іншими відповідними наглядовими органами

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

2. Керівний наглядовий орган може надсилати запит у будь-який час до інших відповідних наглядових органів на надання взаємної допомоги відповідно до статті 61 і може проводити об'єднані операції відповідно до статті 62, зокрема, для здійснення 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 відповідним наглядовим органам. Він повинен без затримки надати проект рішення іншим відповідним наглядовим органам для отримання їхнього висновку та звернути належну увагу на їхні думки.

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

5. Якщо керівний наглядовий орган має намір враховувати висловлене належне та вмотивоване заперечення, він повинен надати іншим відповідним наглядовим органам допрацьований проект рішення для отримання їх висновку. Такий допрацьований проект рішення підлягає процедурі, вказаній у параграфі 4, протягом двотижневого періоду.

6. Якщо жодний з інших відповідних наглядових органів не заперечує щодо проекту рішення, поданого керівним наглядовим органом, протягом періоду, вказаного в параграфах 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 і повідомляє про рішення до головного або 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 було подано скаргу, повідомляє позивача про рішення.

8. Відступаючи від параграфа 7, якщо скаргу було відхилено чи у ній було відмовлено, наглядовий орган, до якого було 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 дій щодо оператора, повідомляє про це головний або єдиний осідок контролера або оператора на території своєї держави-члена та повідомляє про це позивача, в той час як наглядовий орган позивача ухвалює рішення щодо частини, що стосується відхилення чи відмови в такій заяві, та повідомляє про це такому позивачу та інформує про це контролера або оператора.

10. Після отримання повідомлення про рішення керівного наглядового органу відповідно до параграфів 7 і 9, контролер або оператор вживають необхідних заходів для забезпечення відповідності рішенню в тому, що стосується опрацювання даних в контексті всіх його осідків в Союзі. Контролер або оператор повідомляють про заходи, вжиті для відповідності рішенню, керівний наглядовий орган, який повідомляє інші відповідні наглядові органи.

11. Якщо, за виняткових обставин, відповідний наглядовий орган має причини вважати, що є нагальна потреба вживати дії для захисту інтересів суб'єктів даних, застосовують екстрену процедуру, вказану в статті 66.

12. Керівний наглядовий орган і інші відповідні 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 живають заходів для результативної співпраці один з одним. Взаємна допомога охоплює, зокрема, інформаційні запити та заходи щодо нагляду, такі як запити на видачу попередніх дозволів і проведення попередніх консультацій, інспекцій і розслідувань.

2. Кожний наглядовий орган вживає всіх необхідних заходів, необхідних для відповіді на запит іншого наглядового органу без необґрунтованої затримки та не пізніше одного місяця після отримання запиту. Такі заходи можуть включати, зокрема, передавання відповідної інформації щодо проведення 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 надавали запит.

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

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

(b) задоволення запиту може порушити положення 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, прогрес заходів, вжитих для відповіді на запит. Наглядовий орган, до якого надійшов запит, повинен надати інформацію про причини будь-якої відмови в задоволенні запиту відповідно до параграфа 4.

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

7. Наглядові органи, яким надійшли запити, не стягують плати за будь-яку дію, яку вони застосовують згідно із запитом на взаємну допомогу. Наглядові органи можуть узгоджувати правила для відшкодування один одному за окремі витрати, що випливають з надання взаємної допомоги за виняткових обставин.

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

9. Комісія може, шляхом ухвалення імплементаційних актів, визначити формат і процедури взаємної допомоги, вказаної в цій статті, та домовленості для обміну інформацією електронними засобами між наглядовими органами та між наглядовими органами та Радою,

зокрема стандартний формат, вказаний у параграфі 6 цієї статті. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, вказаної в статті 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 члени 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 статтею 56(1) або (4), запрошує наглядовий орган кожної з таких держав-членів брати участь в спільних операціях і відповідає без затримки на запит щодо участі від наглядового органу.

3. Наглядовий орган може, згідно з законом держави-члена, та з дозволу наглядового органу, що направляє, надавати повноваження, в тому числі, слідчі повноваження на членів або персонал наглядового органу, що направляє, залучених до спільних операцій чи, мірою, якою це дозволено законодавством держави-члени за місцем перебування наглядового органу, дозволяти членам чи персоналу наглядового органу, що направляє, реалізовувати їхні слідчі повноваження згідно з законодавством держави-члена наглядового органу, що направляє. 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 направляє, підпорядковуються законодавству держави-члена наглядового органу за місцем перебування.

4. Якщо, згідно з параграфом 1, персонал наглядового органу, що направляє, 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 було нанесено шкоду, виправляє її на умовах, які застосовують до нанесення шкоди її власним персоналом. Держава-член наглядового органу, що направляє, 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 параграфа 5, кожна держава-член повинна утримуватися, у ситуації, передбаченій параграфом 1, від вимоги відшкодування від іншої держави-члена щодо шкоди, вказаної в параграфі 4.

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

Секція 2

Послідовність

Стаття 63

Механізм послідовності

Для того, 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, за яким компетентний наглядовий орган має намір ухвалити будь-який з інструментів, зазначених нижче. З цією метою компетентний наглядовий орган повідомляє проект рішення Ради, якщо воно:

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

(b) стосується питання відповідно до статті 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 статтею 41(3) чи органу сертифікації згідно зі статтею 43(3);

(d) спрямоване на визначення стандартних положень щодо захисту даних, вказаних у пункті (d) статті 46(2) та в статті 28(8);

(e) спрямоване на надання дозволу на договірні положення, вказані в пункті (a) статті 46(3); чи

(f) спрямоване на ухвалення зобов'язальних корпоративних правил у значенні статті 47;

2. Будь-який наглядовий орган, Голова Ради чи Комісія можуть направити 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 дотримується обов'язків щодо взаємної допомоги згідно зі статтею 61 або щодо об'єднаних операцій згідно зі статтею 62.

3. У випадках, вказаних у параграфах 1 і 2, Рада ухвалює висновок з питання, поданого до неї, за умови, що вона не ухвалила раніше висновок з того самого питання. Такий висновок ухвалюють протягом восьми тижнів простою більшістю голосів членів Ради. Цей період може бути подовжено на наступні шість тижнів, беручи до уваги складність предмету. Стосовно проекту рішення, вказаного в параграфі 1, що розіслано членам Ради відповідно до параграфа 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 засобів, з використанням стандартного формату, будь-яку належну інформацію, в тому числі, залежно від обставин короткий виклад фактів, проект рішення, підстави, що викликають необхідність вжиття такого заходу, та погляди інших відповідних наглядових органів.

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

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

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

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

7. Наглядовий орган, вказаний у параграфі 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 або чи вносить зміни та доповнення до її проекту рішення та, якщо такі будуть, проект рішення зі внесеними змінами та доповненнями, з використанням стандартного формату.

8. Якщо відповідний наглядовий орган інформує Голову Ради протягом періоду, вказаного в параграфі 7 цієї статті, що він не має наміру враховувати висновок Ради, в цілому чи частково, надаючи відповідні підстави, у такому разі застосовують статтю 65(1).

Стаття 65

Врегулювання спорів Радою

1. Для того, щоб забезпечити точне і послідовне застосування цього Регламенту в індивідуальних випадках, Рада ухвалює зобов'язальне рішення в таких випадках:

(a) якщо, в ситуації, вказаній в статті 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 необґрунтоване. Зобов'язальне рішення стосується всіх питань, що є предметом належного та обґрунтованого заперечення, зокрема того, чи існують порушення цього Регламенту;

(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 висновок Ради у ситуаціях, вказаних у статті 64(1), або не враховує висновок Ради, ухвалений згідно зі статтею 64. У такому разі, будь-який відповідний наглядовий орган або Комісія може направити питання на розгляд Раді.

2. Рішення, зазначене в параграфі 1, ухвалюють протягом одного місяця з дати направлення предмету більшістю в дві третини голосів членів Ради. Цей період може бути подовжено на наступний місяць, зважаючи на складність суті питання. Рішення, вказане в параграфі 1, повинно бути вмотивованим і адресованим до керівного наглядового органу та всіх відповідних наглядових органів та бути зобов'язальним для них.

3. Якщо Рада не змогла ухвалити рішення протягом періодів, вказаних у параграфі 2, вона повинна ухвалити своє рішення протягом двох тижнів після закінчення другого місяця, вказаного в параграфі 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 параграфом 1, протягом періодів, вказаних у параграфах 2 і 3.

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

6. Керівний наглядовий орган або, залежно від ситуації, наглядовий орган, до якого було подано скаргу, ухвалює своє остаточне рішення на підставі рішення, вказаного в параграфі 1 цієї статті, без необґрунтованої затримки та щонайменше протягом одного місяця після того, як Рада повідомила про своє рішення. Керівний наглядовий орган або, залежно від ситуації, наглядовий орган, до якого було подано скаргу, інформує Раду про дату, коли його остаточне рішення повідомлено, відповідно, контролеру або оператору та суб'єкту даних. Остаточне рішення відповідних наглядових органів ухвалюють на умовах статті 60(7), (8) і (9). Остаточне рішення повинно базуватися на рішенні, вказаному в параграфі 1 цієї статті, та уточнювати, що рішення, вказане в тому параграфі, буде опубліковано на сторінці Ради в мережі Інтернет відповідно до параграфа 5 цієї статті. Остаточне рішення додають до рішення, вказаного в параграфі 1 цієї статті.

Стаття 66

Екстрена процедура

1. За виняткових обставин, якщо залучений наглядовий орган вважає, що існує нагальна потреба вжити дії для захисту інтересів суб'єктів даних, він може, шляхом застосування відступу від механізму послідовності, вказаного в статтях 63, 64 і 65, або процедури, вказаної в статті 60, негайно вжити тимчасових заходів, спрямованих на породження юридичних наслідків на своїй власній території з уточненим строком дійсності, що не перевищує три місяці. Наглядовий орган повинен, без затримки, повідомити про такі заходи та причини їх прийняття іншим відповідним наглядовим органам, Раді та Комісії.

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

3. Будь-який наглядовий орган може направляти 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 є нагальна потреба діяти, для того, щоб захистити права та свободи суб'єктів даних, надаючи інформацію про причини для запиту на такий висновок чи рішення, в тому числі, для нагальної потреби діяти.

4. Відступаючи від статті 64(3) і статті 65(2), терміновий висновок чи термінове зобов'язальне рішення, вказані в параграфах 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 статті 64.

Такі імплементаційні акти ухвалюють відповідно до експертної процедури, вказаної в статті 93(2).

Секція 3

Європейська рада із захисту даних

Стаття 68

Європейська рада із захисту даних

1. Цим засновується 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 їхніх відповідних представників.

4. Якщо в державі-члені понад один наглядовий орган несе відповідальність за моніторинг застосування положень згідно з цим Регламентом, 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, вказаних у статті 65, Європейський інспектор із захисту даних володіє правом голосу лише щодо рішень, що стосуються принципів і правил, застосовних до установ, органів, служб і агентств Союзу, які по суті відповідають принципам і нормам цього Регламенту.

Стаття 69

Незалежність

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

2. Без обмеження запитів Комісії, вказаних у пункті (b) статті 70(1) та статті 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, за власною ініціативою, або, за необхідності, на запит Комісії, зокрема:

(a) здійснює моніторинг і забезпечує правильне застосування цього Регламенту у випадках, передбачених статтями 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, з 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 щодо зобов'язальних корпоративних правил;

(d) видає настанови, рекомендації та інформацію про кращу практику щодо процедур для стирання посилань, копій чи накладів персональних даних із загальнодоступних послуг зв'язку, вказаних у статті 17(2);

(e) розглядає, за власною ініціативою, на запит одного з її членів або на запит Комісії, будь-яке питання, що охоплює застосування цього Регламенту та видає настанови, рекомендації та інформацію про кращу практику для того, щоб заохотити послідовне застосування цього Регламенту;

(f) видає настанови, рекомендації та інформацію про кращу практику згідно з пунктом (e) цього параграфа для подальшого визначення критеріїв і умов для рішень, що ґрунтуються на профайлінгу відповідно до статті 22(2);

(g) видає настанови, рекомендації та інформацію про кращу практику згідно з пунктом (e) цього параграфа для встановлення порушень захисту персональних даних і визначення неналежної затримки, вказаної в статті 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 кращу практику згідно з пунктом (e) цього параграфа щодо обставин, за яких порушення захисту персональних даних ймовірно створюватиме високий ризик для прав і свобод фізичних осіб, вказаних у статті 34(1).

(i) видає настанови, рекомендації та інформацію про кращу практику згідно з пунктом (e) цього параграфа з метою подальшого визначення критеріїв і вимог для передавання персональних даних на підставі зобов'язальних корпоративних правил, яких дотримуються контролери, і зобов'язальних корпоративних правил, яких дотримуються оператори, а також подальших вимог, необхідних для забезпечення захисту персональних даних залучених суб'єктів даних, вказаних у статті 47;

(j) видає настанови, рекомендації та інформацію про кращу практику згідно з пунктом (e) цього параграфа для подальшого уточнення критеріїв і вимог для передавання персональних даних на підставі статті 49(1);

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

(l) переглядає практичне застосування настанов, рекомендацій і прикладів кращої практики, вказаних у пунктах (e) і (f);

(m) видає настанови, рекомендації та інформацію про кращу практику згідно з пунктом (e) цього параграфа для запровадження спільних процедур через звітування фізичними особами про порушення цього Регламенту згідно зі статтею 54(2);

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

(o) проводить акредитацію органів сертифікації, здійснює періодичний перегляд відповідно до статті 43, веде публічний реєстр акредитованих органів відповідно до статті 43(6) та акредитованих контролерів або операторів, які мають свої осідки в третіх країнах згідно зі статтею 42(7);

(p) визначає вимоги, вказані в статті 43(3), для акредитації органів сертифікації згідно зі статтею 42;

(q) надає Комісії висновок щодо вимог до сертифікації, вказаних у статті 43(8);

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

(s) надає Комісії висновок для оцінювання належного рівня захисту в третій країні чи міжнародній організації, в тому числі для оцінювання, чи не забезпечує більше 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, вказаного в статті 64(1), щодо питань, поданих відповідно до статті 64(2), та видає зобов'язальні рішення відповідно до статті 65, у тому числі у випадках, вказаних у статті 66;

(u) заохочує співпрацю та ефективний двосторонній і багатосторонній обмін інформацією та кращою практикою між наглядовими органами;

(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 практикою з органами нагляду за захистом даних у всьому світі.

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

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

2. Якщо Комісія надає запит на консультацію Ради, вона може вказати часове обмеження, беручи до уваги терміновий характер питання.

3. Рада передає свої висновки, настанови, рекомендації та інформацію про кращу практику Комісії та комітету, вказаному в статті 93, і опубліковує їх.

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

Стаття 71

Звіти

1. Рада складає річний звіт щодо захисту 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 кращої практики, вказаних у пункті (i) статті 70(1), а також зобов'язальних рішень, вказаних у статті 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 та двох заступників голови з числа її членів простою більшістю.

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

Стаття 74

Завдання Голови

1. Голова має такі завдання:

(a) скликати засідання Ради та готувати його порядок денний;

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

(c) забезпечувати вчасне виконання завдань Ради, зокрема, щодо механізму послідовності, вказаного в статті 63.

2. Рада встановлює розподіл завдань 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 окремий механізм підзвітності від персоналу, залученого до виконання завдань, покладених на Європейського інспектора із захисту даних.

4. За необхідності, Рада і Європейський інспектор із захисту даних готують та опубліковують Меморандум про взаєморозуміння для імплементації цієї статті, визначаючи умови їхньої 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 та виконання за результатами зустрічей Ради;

(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 за необхідне, як передбачено в її правилах процедури.

2. Доступ до документів, поданих до членів Ради, експертів і представників третіх сторін, регулюється Регламентом Європейського Парламенту і Ради (ЄС) № 1049/2001 ([1]).

ГЛАВА 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 порушує положення цього Регламенту.

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

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 проти 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, що є компетентним відповідно до статей 55 і 56, не розглядає скаргу або не інформує суб'єкта даних протягом трьох місяців про стан і результати розгляду скарги, поданої відповідно до статті 77.

3. Провадження щодо наглядового органу здійснюють в судах держави-члена, де засновано наглядовий орган.

([1]) Регламент Європейського Парламенту і Ради (ЄС) № 1049/2001 від 30 травня 2001 року про публічний доступ до документів Європейського Парламенту, Ради і Комісії (ОВ L 145, 31.05.2001, с. 43).

4. Якщо провадження здійснюють щодо рішення наглядового органу, якому передували висновок або рішення Ради за механізмом послідовності, наглядовий орган перенаправляє 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 статті 77, кожний суб'єкт даних повинен мати право на дієвий судовий засіб правового захисту, якщо він вважає, що його права за цим Регламентом було порушено внаслідок опрацювання його персональних даних, що не відповідає цьому Регламенту.

2. Провадження щодо контролера або оператора здійснюють в судах держави-члена, де 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 рамках 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, вказані в статтях 77, 78 і 79 від його або її імені, та реалізовувати право на отримання відшкодування, вказане в статті 82, від його або її імені, як це передбачено законодавством держави-члена.

2. Держави-члени можуть передбачити, щоб будь-який орган, організація чи асоціація, вказані в параграфі 1 цієї статті, мали право подати скаргу в такій державі-члені, до наглядового органу, що є компетентним відповідно до статті 77, і реалізовувати права, вказані в статтях 78 і 79, якщо вважає, що права суб'єкта даних за цим Регламентом було порушено в результаті опрацювання.

Стаття 81

Призупинення провадження

1. Якщо компетентний суд держави-члена володіє інформацією про провадження щодо того самого питання, що стосується опрацювання тим самим контролером або оператором, яке здійснюють в 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, що стосується опрацювання тим самим контролером або оператором, здійснюють в 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 в результаті 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 порушує положення цього Регламенту. Оператор несе відповідальність за шкоду, заподіяну опрацюванням лише тоді, коли він не дотримується обов'язків за цим Регламентом, спрямовані безпосередньо на оператора, або якщо він діє поза чи всупереч законним вказівкам контролера.

3. Контролер або оператор звільняються від відповідальності за параграфом 2, якщо доведуть, що жодним чином не несуть відповідальності за подію, що спричиняє нанесення шкоди.

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

5. Якщо контролер або оператор, відповідно до параграфа 4, виплатили повне відшкодування за 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, встановлених у параграфі 2.

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

Стаття 83

Загальні умови для накладання адміністративних штрафів

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

2. Адміністративні штрафи, залежно від обставин кожного окремого випадку, накладають як доповнення до, чи замість, заходів, вказаних у пунктах (a)-(h) і (j) статті 58(2). Під час вирішення, чи накладати адміністративний штраф, і вирішення щодо розміру адміністративного штрафу в кожному окремому випадку необхідно звертати належну увагу на 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 рівень шкоди, заподіяної їм;

(b) навмисний або недбалий характер порушення;

(c) будь-які дії, 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 статей 25 і 32;

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

(f) рівень співпраці з наглядовим органом для відшкодування порушення і скорочення можливих негативних наслідків порушення;

(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, вказані в статті 58(2), було раніше призначено проти відповідного контролера або оператора щодо того самого питання, — відповідність цим заходам;

(j) дотримання затверджених кодексів поведінки відповідно до статті 40 або затверджених кодексів поведінки відповідно до статті 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, від порушення.

3. Якщо контролер або оператор навмисно чи за недбалістю, для 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 параграфом 2, поширюється застосування адміністративних штрафів сумою до 10 000 000 євро або, у випадку підприємства, до 2% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою:

(a) обов'язки контролер і оператора відповідно до статей 8, 11, 25–39, і 42, і 43;

(b) обов'язки органу з сертифікації відповідно до статей 42 і 43;

(c) обов'язки органу з моніторингу відповідно до статті 41(4);

5. На порушення таких положень, згідно з параграфом 2, поширюється застосування адміністративних штрафів сумою до 20 000 000 євро або, у випадку підприємства, до 4% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою:

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

(b) права суб'єктів даних відповідно до статей 12–22;

(c) акти передавання персональних даних до одержувача в третій країні чи до міжнародної організації відповідно до статей 44–49;

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

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

6. На невідповідність постанові наглядового органу, як вказано в статті 58(2), згідно з параграфом 2 цієї статті, поширюється застосування адміністративних штрафів сумою до 20 000 000 євро або, у випадку підприємства, до 4% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою.

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

8. Реалізація наглядовим органом своїх повноважень за цією статтею 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, які накладають наглядові органи. 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 до цієї глави, до 25 травня 2018 року та, без затримки, про будь-які подальші зміни і доповнення, що на них впливають.

Стаття 84

Санкції

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

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

ГЛАВА 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 та свободу інформації, в тому числі, опрацювання для цілей журналістики та цілей наукової, художньої чи літературної діяльності.

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

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

Стаття 86

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

Стаття 87

Опрацювання національного ідентифікаційного номеру

Держави-члени можуть в подальшому визначити особливі умови для опрацювання національного ідентифікаційного номеру 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, установлених законом або колективними угодами, управління, планування та організацію праці, рівність та різноманітність на робочому місці, здоров'я та безпеку 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 для захисту людської гідності суб'єкта даних, законних інтересів і фундаментальних прав, з особливим урахуванням прозорості опрацювання, передавання персональних даних у межах групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, та систем моніторингу на робочому місці.

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

Стаття 89

Гарантії та відступи, що стосуються опрацювання для досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження або статистичних цілей

1. Опрацювання для досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження або статистичних цілей підлягає застосуванню 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 умови можливості досягнути у такий спосіб зазначених цілей. Якщо таких цілей можна досягнути у ході подальшого опрацювання, що не дозволяє чи більше не дозволяє ідентифікацію 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 відступи від прав, вказаних у статтях 15, 16, 18 і 21 з урахуванням умов і гарантій, вказаних у параграфі 1 цієї статті, якщо такі права ймовірно унеможливлять або серйозно обмежать досягнення спеціальних цілей, і такі відступи є необхідними для досягнення таких цілей.

3. Якщо персональні дані опрацьовують для досягнення цілей суспільного інтересу, законодавство Союзу або держави-члена може передбачати відступи від прав, вказаних у статтях 15, 16, 18 і 21 з урахуванням умов і гарантій, вказаних у параграфі 1 цієї статті, якщо такі права ймовірно унеможливлять або серйозно обмежать досягнення спеціальних цілей, і такі відступи є необхідними для досягнення таких цілей.

4. Якщо опрацювання, вказане в параграфах 2 і 3, слугує водночас іншій цілі, відступи застосовують лише до опрацювання для цілей, вказаних у тих параграфах.

Стаття 90

Обов'язки збереження таємниці

1. Держави-члени можуть ухвалювати спеціальні норми для визначення повноважень наглядових органів, установлених у пунктах (e) і (f) статті 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 є необхідним і пропорційним для узгодження права на захист персональних даних із обов'язком збереження таємниці. Такі норми застосовують лише щодо персональних даних, які отримав контролер або оператор у результаті чи під час діяльності, на яку поширюється такий обов'язок збереження таємниці.

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

Стаття 91

Чинні правила захисту даних церков і релігійних асоціацій

1. Якщо в державі-члені, церкви та релігійні асоціації 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 приведення їх у відповідність з цим Регламентом.

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

ГЛАВА X

Делеговані акти та імплементаційні акти

Стаття 92

Здійснення делегування

1. Повноваження для ухвалення делегованих актів надаються Комісії з дотриманням умов, установлених у цій статті.

2. Делеговані повноваження, зазначені в статті 12(8) і статті 43(8), надаються Комісії на невизначений період часу, починаючи з 24 травня 2016 року.

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

4. Як тільки Комісія ухвалює делегований акт, вона надає його одночасно Європейському Парламенту і Раді.

5. Делегований акт, ухвалений відповідно до статті 12(8) і статті 43(8), набуває чинності тільки в тому випадку, якщо ні Європейський Парламент, ні Рада не висловили жодних заперечень протягом тримісячного періоду з дати надання зазначеного акта Європейському Парламенту і Раді, або, якщо до закінчення такого періоду і Європейський Парламент і Рада повідомили Комісію про те, що не матимуть заперечень. Такий період подовжується ще на три місяці за ініціативою 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 параграф необхідно застосовувати статтю 5 Регламенту (ЄС) № 182/2011.

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

ГЛАВА XI

Прикінцеві положення

Стаття 94

Скасування Директиви 95/46/ЄС

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

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, засновану статтею 29 Директиви 95/46/ЄС, необхідно тлумачити як покликання на Європейську Раду із захисту даних, засновану 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 року та які 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 року та кожні чотири роки після цієї дати, Комісія подає звіт щодо оцінювання та перевірки виконання цього Регламенту до Європейського Парламенту та Ради. Звіти необхідно оприлюднити.

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

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

(b) Глави VII про співпрацю і послідовність.

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

4. Проводячи оцінювання та перевірки, вказані в параграфах 1 та 2, Комісія бере до уваги 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 та ступінь 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 руху таких даних.

Стаття 99

Набуття чинності та застосування

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

2. Він застосовується з 25 травня 2018 року.

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

Вчинено в Брюсселі 27 квітня 2016 року.

За Європейський Парламент	*За Раду*
Президент	*Президент*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT