І

*(Акти, публікація яких є обов’язковою)*

# РЕГЛАМЕНТ (ЄС) № 45/2001 ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ ТА РАДИ

# від 18 грудня 2000 року

**стосовно захисту осіб з точки зору обробки персональних даних установами та органами Спільноти та вільного руху таких даних**

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ ТА РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про заснування Європейських Спільнот, а саме Статтю 286 цього Договору,

Беручи до уваги пропозицію від Комісії (1),

Беручи до уваги думку Комітету з економічних та соціальних питань (2),

Діючи згідно з процедурою, викладеною у Статті 251 Договору (3),

Оскільки:

1. Стаття 286 Договору вимагає надання в органи та установи Спільноти актів по захисту осіб щодо обробки персональних даних та вільного руху таких даних.
2. Повністю сформована система захисту персональних даних не лише вимагає встановлення прав суб’єктів даних та зобов’язань для тих, хто обробляє ці персональні дані, але також доречні санкції до порушників та моніторинг незалежним органом нагляду.
3. Стаття 286(2) Договору вимагає встановлення незалежного наглядового органу, який відповідає за моніторинг виконання таких актів Спільноти у закладах та органах Спільноти.
4. Стаття 286(2) Договору вимагає прийняття будь-яких інших доречних положень.

(1) OJ C 376E, 28.12.1999, с. 24.

(2) OJ C 51, 23.2.2000, с. 48.

1. Регламент є необхідним для надання особам прав, що підтримуються законом, для визначення зобов’язань контролерів у межах установ та органів Спільноти, а також для створення незалежного наглядового органу для моніторингу обробки персональних даних установами та органами Спільноти.
2. Була проведена консультація з Робочою групою з захисту осіб щодо обробки персональних даних, встановленою згідно зі Статтею 29 Директиви 95/46/ЄС Європейського парламенту та Ради від 24 жовтня 1995 року стосовно захисту осіб щодо обробки персональних даних та вільного руху таких даних (4).
3. Особами, які підлягають захисту, являються ті, чиї дані обробляються установами та органами Спільноти у будь-якому контексті, наприклад, ці особи працюють у цих установах та органах.
4. Принципи захисту даних мають застосовуватися до будь-якої інформації, що стосується ідентифікованої особи, або особи, яку можна ідентифікувати. Щоб визначити, чи можна ідентифікувати особу, необхідно брати до уваги усі засоби, які можуть бути розумно застосовані контролером або будь-якою іншою особою для ідентифікації згаданої особи. Принципи захисту не застосовуються до даних, що надаються анонімно, та таким чином, що суб’єкт даних не можливо ідентифікувати.
5. Директива 95/46/ЄС вимагає, щоб держави-члени охороняли фундаментальні права та свободи осіб, у томі числі їх право на приватність з точки зору обробки персональних даних, щоб забезпечити вільний потік персональних даних у Спільноті.

(3) Думка Європейського парламенту від 14 листопада 2000 року та

Рішення Ради від 30 листопада 2000 року. (4) OJ L 281, 23.11.1995, с. 31.

1. Директива 97/66/ЄС Європейського парламенту та Ради від 15 грудня 1997 року стосовно обробки персональних даних та захисту приватності у секторі телекомунікацій (1) конкретизує та доповнює Директиву 95/46/ЄС з точки зору обробки персональних даних у секторі телекомунікацій.
2. Також розробляються різні заходи у межах Спільноти, включаючи заходи щодо взаємної допомоги між національними органами та Комісією, які також обумовлюють та доповнюють Директиву 95/46/ЄС по секторам, до яких вони відносяться.
3. Послідовне та однорідне застосування правил захисту фундаментальних прав та свобод особи відносно обробки персональних даних мають бути забезпечені у всій Спільноті.
4. Метою є забезпечення ефективної відповідності правилам, що керують захистом фундаментальних прав та свобод особи, та вільним потоком персональних даних між державами-членами та установами і органами Спільноти або між установами і органами Спільноти з цілями, які пов’язані з виконанням їх відповідних компетенцій.
5. З цього приводу необхідно прийняти заходи, закріплені за установами та органами Спільноти. Ці заходи мають бути застосовані до усіх процесів обробки персональних даних усіма установами та органами Спільноти в такої мірі, щоб ці процеси обробки проводилися таким чином, що вони суцільно або частково підпадали під законодавство Спільноти.
6. У випадках, коли така обробка проводиться установами або органами Спільноти з використанням видів діяльності, що не підпадають під цей Регламент, а саме вказані у Частині V та VI Договору Європейського союзу, захист фундаментальних прав та свобод особи має забезпечуватися відповідно до Статті 6 Договору Європейського союзу. Доступ до документів, включаючи умови доступу до документів з персональними даними, регулюється правилами, прийнятими на основі Статті 225 Договору ЄС, яка охоплює Частини V та VI Договору Європейського союзу.
7. Заходи не застосовуються до органів, створених поза межами структури Спільноти, та європейський інспектор із захисту даних не має бути компетентним у контролі обробки персональних даних такими органами.
8. Ефективність захисту осіб з урахуванням обробки персональних даних у Союзі передбачає послідовність відповідних правил та процедур, що застосовуються до видів діяльності, що належать до різних юридичних контекстів. Розробка фундаментальних принципів захисту персональних даних у сферах

(1) OJ L 24, 30.1.1998, с. 1.

юридичної взаємодії по кримінальних справах та взаємодії поліції та митниці, а також створення секретаріату для сумісних органів нагляду та контролю було встановлено Конвенцією Європолу, Конвенція по використанню інформаційних технологій для митних цілей та Шенгенська Конвенція представляють собою перший крок у цьому напрямку.

1. Цей Регламент не повинен впливати на права та зобов’язання держав-членів згідно з Директивами 95/4ЄС та 966/ЄС. Не існує наміру змінити існуючі процедури та практики, що законно застосовуються державами-членами у сфері національної безпеки, запобігання заворушенням або запобігання, визначення, розслідування та переслідування кримінальних порушень, згідно з Протоколом про привілеї та імунітети Європейських Спільнот та міжнародному закону.
2. Установи та органи Спільноти мають інформувати компетентні органи у державах-членах, коли вони вважають, що комунікації у їхніх телекомунікаційних мережах необхідно перехопити, згідно з відповідними національними положеннями.
3. Положення, що застосовуються до установ та органів Спільноти мають відповідати положенням, викладеним у зв’язку з гармонізацією національних законів або імплементації іншої політики Спільноти, особливо у сфері взаємної допомоги. Однак, може бути важливим визначити та доповнити ці положення, коли йдеться про забезпечення захисту у випадку обробки персональних даних установами та органами Спільноти.
4. Це стосується прав осіб, чиї дані обробляються, зобов’язань установ та органів Спільноти, що проводять обробку, та прав, що надаються незалежному наглядовому органу, який несе відповідальність за забезпечення правильної імплементації цього Регламенту.
5. Права, надані суб’єкту даних, та дії внаслідок цих прав не мають впливати на зобов’язання, покладені на контролера.
6. Незалежний наглядовий орган має застосовувати свої наглядові функції згідно з Договором та відповідно до прав людини та фундаментальних свобод. Цей орган має проводити запити відповідно до Протоколу з привілеїв та імунітету та з Регламентами стосовно персоналу посадових осіб Європейських Спільнот, а також згідно з умовами зайнятості, що застосовуються до інших службовців Спільнот.
7. Приймаються необхідні технічні засоби, щоб відкрити доступ до реєстрів процесів обробки, що проводяться із відповідальними з питань захисту даних через незалежні наглядові органи.
8. Рішення незалежного наглядового органу стосовно пільг, гарантій, авторизації та умов, що стосуються операцій обробки даних, як визначено цим Регламентом, мають бути опубліковані у звітах діяльності. Незалежно від публікації щорічного звіту діяльності, незалежний наглядовий орган може опублікувати звіти з конкретних питань.
9. Певні процеси обробки, які можуть спричинити ризики стосовно прав та свобод суб’єктів даних, підлягають попередній перевірці незалежним наглядовим органом. Думка, отримана в контексті попередньої перевірки, включаючи думку, отриману у результаті неотримання відповіді за період часу, є підставою для подальших дій з боку незалежного наглядового органу відносно процесу обробки про який йде мова.
10. Обробка персональних даних для виконання завдань, що виконуються установами та органами Спільноти в інтересах держави, включають обробку персональних даних для управління та функціонування тих установ та органів.
11. У певних випадках обробка даних може бути дозволена положеннями Спільноти або актами, що замінюють положення Спільноти. Однак, у перехідний період, коли такі положення не існують, очікуючи прийняття, Європейський інспектор із захисту даних може дозволити обробку таких даних за умови, що будуть надані доречні засоби захисту. Приймаючи таке рішення, він має брати до уваги положення, прийняті державою-членом для роботи з подібними випадками.
12. Ці випадки стосуються обробки даних, що розкриває расову чи етнічну приналежність, політичні погляди, релігійні або філософські вірування або належність до профспілки, та обробки даних, що стосуються здоров’я або інтимного життя, які є важливими для виконання певних прав та зобов’язань контролера у сфері трудового законодавства або с причин, що є важливими для державних інтересів. Вони також стосуються обробки даних щодо порушень, судимостей або заходів безпеки та авторизації, для застосування рішення до суб’єкту даних, що створює юридичні ефекти, які стосуються його

або її або суттєво впливає на нього або неї, та які базуються лише на автоматичній обробці даних, спрямованих на оцінювання певних персональних аспектів, що відносяться до нього або неї.

1. Може виникнути необхідність проводити моніторинг комп’ютерних мереж, що працюють під контролем установ та органів Спільноти, з метою запобігання неавторизованому використанню. Європейський інспектор із захисту даних має визначити, при яких умовах це є можливим.
2. Відповідальність, що виходить з будь-якого порушення цього Регламенту, урегульовується другим параграфом Статті 288 Договору.
3. У кожній установі або органі Спільноти щонайменше один спеціаліст з захисту даних має забезпечувати, що положення цього Регламенту виконуються, та має надавати поради контролерам стосовно виконання їхніх зобов’язань.
4. Згідно зі Статтею 21 Регламенту Ради (ЄС) № 322/97 від 17 лютого 1997 року стосовно Статистики Спільноти (1), Регламент має застосовуватися без обмежень Директиви 95/46/ЄС.
5. Згідно зі Статтею 8(8) Регламенту Ради (ЄС) № 2533/98 від 23 листопада 1998 року стосовно збору статистичної інформації Центральним європейським банком (2), Регламент має застосовуватися без обмежень Директиви 95/46/ЄС.
6. Згідно зі Статтею 1(2) Регламенту Ради (Євратом, ЕЕС) № 1588/90 від 11 червня 1990 року стосовно передачі даних, що є предметом статистичної конфіденційності, до Офісу статистики Європейських Спільнот (3), Регламент не зменшує спеціальні положення Спільноти або національні положення стосовно захисту конфіденційності, окрім статистичної конфіденційності.
7. Цей Регламент не має на меті обмежити простір для маневру для держав-членів у прийнятті їх власних законів щодо захисту даних згідно зі Статтею 32 Директиви 95/46/ЄС у відповідності зі Статтею 249 Договору,

ПРИЙНЯЛИ ЦЕЙ РЕГЛАМЕНТ:

ГЛАВА 1

# ЗАГАЛЬНІ ПОЛОЖЕННЯ

*Стаття 1*

# Об’єкт Регламенту

* 1. Згідно з цим Регламентом, заклади та органи, створені за допомогою, або на основі Договорів про заснування Європейських Спільнот, надалі "Органи або установи Спільноти",

(1) OJ L 52, 22.2.1997, с. 1.

(2) OJ L 318, 27.11.1998, с. 8.

(3) OJ L 151, 15. 6.1990, с. 1. Регламент, доповнений Регламентом (ЄС) (322/97 (OJ L 52, 22.2.1997, с. 1).

захищатимуть фундаментальні права та свободи осіб, а саме їх право на приватність з точки зору обробки персональних даних, та не будуть обмежувати та забороняти вільний потік персональних даних між ними або одержувачами згідно з національним законом держав-членів, що впроваджують Директиву 95/46/ЄС.

* 1. Незалежний наглядовий орган, створений згідно з цим Регламентом, надалі "Європейський інспектор із захисту даних", контролюватиме застосування положень цього Регламенту до усіх операцій обробки, які проводяться установою або органом Спільноти.

*Стаття 2*

# Визначення

Для цілей цього Регламенту:

1. "персональні дані" означають інформацію, що стосується ідентифікованої фізичної особи, або такої, що не може бути ідентифікованою, надалі "суб’єкт даних"; особа, що може бути ідентифікована, це особа, яка може ідентифікована прямо або опосередковано, а саме посиланням на ідентифікаційний номер або на один або більше факторів, які є специфічними для його або її фізичної, фізіологічної, психологічної, економічної, культурної або соціальної особистості;
2. "обробка персональних даних", надалі "обробка" означає процедуру або набір процедур, які виконуються з персональними даними, автоматичними або не автоматичними засобами, такі як збір, запис, організація, збереження, адаптування або перебудова, пошук, консультація, використання, розкриття через передачу, розповсюдження або розкриття іншими способами, групування або комбінування, блокування, стирання або знищення;
3. "інформаційна система персональних даних", надалі "інформаційна система" означає будь-який структурований набір персональних даних, доступ до яких отримується згідно з певними критеріями, чи централізовано, чи децентралізовано або розподілений на функціональній або географічній основі;
4. "контролер" означає установу або орган Спільноти, Генеральний Директорат, підрозділ або іншу установу, яка самостійно або сумісно з іншими визначає цілі та засоби обробки персональних даних; де цілі та засоби обробки даних визначаються спеціальним актом Спільноти, контролер або спеціальні критерії для його призначення можуть бути визначені таким актом Спільноти;
5. "обробник" означає фізичну або юридичну особу, державний орган, агентство або будь-який інший орган, який обробляє персональні дані від імені контролера;
6. "третя сторона" означає фізичну або юридичну особу, державний орган, агентство або будь-який інший орган, що не є суб’єктом даних, контролером, обробником та особами, які мають право на обробку даних під прямим керівництвом контролера або обробника;
7. "реципієнт" означає фізичну або юридичну особу, державний орган, агентство або інший орган, якому надаються дані, незважаючи чи є цей орган третьою стороною; однак, органи, які отримують дані у рамках спеціального запиту не розглядаються як реципієнти;
8. "згода суб’єкту даних" означає вільно надані спеціальні та поінформовані ознаки його або її бажань, якими суб’єкт даних виражає його або її згоду на обробку персональних даних, що стосуються його або її.

*Стаття 3*

# Сфера застосування

1. Цей Регламент має бути застосований до процесів обробки персональних даних усіма установами та органами Спільноти до такої міри, щоб ці процеси обробки проводилися таким чином, що вони суцільно або частково підпадали під законодавство Спільноти.
2. Цей Регламент має бути застосований до обробки персональних даних автоматизованими засобами повністю або частково, а також до обробки персональних даних засобами відмінними від автоматичних, ці персональні дані формують частину інформаційної системи або мають сформувати частину інформаційної системи.

ГЛАВА 2

# ЗАГАЛЬНІ ПРАВИЛА ЗАКОННОСТІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

РОЗДІЛ 1

**ПРИНЦИПИ, ЩО СТОСУЮТЬСЯ ЯКОСТІ ДАНИХ**

*Стаття 4*

# Якість даних

1. Персональні дані мають бути:
2. обробленими чесно та законно;
3. зібраними для вказаних, відкритих та законних цілей, і надалі не можуть бути оброблені у будь-який спосіб, що не відповідає цим цілям. Подальша обробка персональних даних з історичними, статистичними або науковими цілями не може вважатися несумісною за умови, що контролер надає необхідні засоби захисту, а саме, забезпечує, що дані не обробляються для інших цілей або використовуються для підтримки засобів або рішень стосовно певної особи;
4. компетентними, відповідними та не надмірними у відношенні до цілей, з якими вони зібрані та/або надалі обробляються;
5. точними та якщо необхідно актуальними; мають прийматися усі доречні кроки для забезпечення того, що неточні та неповні дані видаляються або виправляються, зважаючи на цілі, з якими вони були зібрані або надалі обробляються;
6. зберігатися у формі, що дозволяє ідентифікацію суб’єктів даних не довше, ніж це є необхідним для досягнення цілей, з якими дані були зібрані або для яких вони обробляються. Установа або орган Спільноти мають затвердити, що персональні дані, які мають зберігатися довший період часу для використання з історичними, статистичними або науковими цілями,слід зберігати або у анонімній формі, або, якщо це неможливо, лише з зашифрованими особистостями суб’єктів даних. У будь-якому випадку, дані не можна використовувати для будь-яких інших цілей, окрім історичних, статистичних або наукових.
7. Саме контролер забезпечує відповідність параграфу 1.

РОЗДІЛ 2

**КРИТЕРІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЛЕГІТИМНОСТІ ОБРОБКИ ДАНИХ**

*Стаття 5*

# Законність обробки

Персональні дані можна обробляти, якщо;

1. обробка необхідна для виконання завдання, що виконується в інтересах держави на основі Договорів про заснування Європейських Спільнот, або інших юридичних інструментах, прийнятих на основі цього, або юридичних актах офіційного органу наданих установі або органу Спільноти, або третій стороні. яким відкриваються дані, або
2. обробка є необхідною, щоб досягнути відповідності законним зобов’язанням, яким підпорядкований контролер, або
3. обробка є необхідною для виконання контракту, учасником якого є суб’єкт даних, або для прийняття мір на запит суб’єкта даних перед підписанням контракту, або
4. суб’єкт даних недвозначно надав/надала свою згоду, або
5. обробка необхідна для захисту важливих інтересів суб’єкту даних.

*Стаття 6*

# Зміна цілі

Без шкоди для Статей 4, 5 та 10:

1. Персональні дані мають оброблятися не тільки для цілей для яких вони були зібрані, якщо зміна цілі чітко дозволена внутрішніми правилами установи або органом Спільноти.
2. Персональні дані, зібрані виключно для забезпечення захисту або контролю систем або процесів обробки даних, не можуть використовуватися для будь-яких інших цілей, за виключенням запобігання, розслідування, визначення або переслідування серйозних кримінальних порушень.

*Стаття 7*

# Передача персональних даних у межах або між установами та органами Спільноти

Без шкоди для Статей 4, 5, 6 та 10:

1. Персональні дані повинні передаватися тільки у межах однієї або до інших установ або органів Спільноти, якщо ці дані є необхідними для законного виконання завдань, що є частиною компетентності реципієнта.
2. У випадках передачі даних на запит реципієнта, і контролер і реципієнт несуть відповідальність за законність такої передачі.

Контролер має підтвердити компетентність реципієнта та зробити попередню оцінку необхідності передачі даних. Якщо виникають сумніви стосовно такої необхідності, контролер шукає додаткову інформацію у реципієнта.

Реципієнт має забезпечити, що необхідність для передачі даних може бути згодом перевірена.

1. Реципієнт має обробляти персональні дані лише з цілями, для яких вони були передані.

*Стаття 8*

# Передача персональних даних реципієнтам, які підпорядковуються Директиві 95/46/ЄС, але не є установами та органами Спільноти

Без шкоди для Статей 4, 5, 6 та 10 персональні дані можуть бути передані лише реципієнтам, які підпорядковуються національним законам, прийнятим для імплементації Директиви 95/46/ЄС,

1. якщо реципієнт встановлює, що дані є необхідними для виконання завдання, що проводиться у державних інтересах, або підпорядковується державним органам, або
2. якщо реципієнт встановлює необхідність передачі даних, та якщо не існує причин припускати, що може бути нанесено шкоду законному праву суб’єкта даних.

*Стаття 9*

# Передача персональних даних реципієнтам, які не підпорядковуються Директиві 95/46/ЄС, та не є установами та органами Спільноти

1. Персональні дані можуть бути передані реципієнтам, що не є установами або органами Спільноти, які не підпорядковуються національному закону, прийнятому згідно з Директивою 95/46/ЄС, якщо відповідний рівень захисту забезпечується у країні реципієнта або у межах міжнародної організації реципієнта, та якщо дані передаються виключно для виконання завдань, які входять до компетенції контролера.
2. Відповідність рівня захисту, що надається третьою країною або міжнародною організацією, має оцінюватися з точки зору обставин, що оточують операцію передачі даних або операцію передачі набору даних; особлива увага приділяється характеру даних, цілям та тривалості запропонованих операцій обробки даних, третій країні реципієнта або міжнародній організації реципієнта, законам, загальним та спеціальним, що є чинними у третій країні або міжнародній організації, та професійним правилам та заходам безпеки, які виконуються у цій третій країні або міжнародній організації.
3. Установи та органи Спільноти мають інформувати Комісію та європейського інспектора із захисту даних про випадки, коли вони вважають, що третя країна або міжнародна організація не забезпечують відповідний рівень захисту у розумінні параграфа 2.
4. Комісія має інформувати держави-члени про будь-які випадки, як зазначено у параграфі 3.
5. Установи та органи Спільноти мають проводити необхідні заходи, щоб відповідати рішенням прийнятим Комісією, коли вони встановлюють, згідно зі Статтею 25(4) та (6) Директиви 95/46/ЄС, що третя країна або міжнародна організація забезпечує або не забезпечує відповідний рівень захисту.
6. При частковому скасуванні параграфів 1 та 2 установи або органи Спільноти можуть передавати персональні дані, якщо:
7. суб’єкт даних недвозначно надав/надала свою згоду на запропоновану передачу; або
8. передача є необхідною для виконання контракту між суб’єктом даних та контролером або для імплементації переддоговірних засобів, що приймаються у відповідь на запит суб’єкта даних; або
9. передача є необхідною для завершення або виконання контракту, введеного в інтересах суб’єкту даних, між контролером та третьою стороною; або
10. передача є необхідною або юридично обґрунтованою на основі важливих державних інтересів, або для встановлення, виконання або захисту правових вимог; або
11. передача необхідна для захисту важливих інтересів суб’єкту даних; або
12. передача проводиться з реєстру, який, згідно з законом Спільноти, спрямований на надання інформації широкому загалу, та який відкритий для звернень з боку громадськості взагалі або будь-якою особою, яка демонструє законний інтерес, до ступеня коли по певному випадку виконуються умови, викладені у законі Спільноти стосовно звернень.
13. Без шкоди для параграфу 6, європейський інспектор із захисту даних може дозволити передачу або набір персональних даних третій країні або міжнародній організації, яка не забезпечує відповідний рівень захисту у межах параграфів 1 та 2, коли контролер посилається на доречні запобіжні заходи для захисту приватності та фундаментальних прав та свобод особистостей, та виконання відповідних прав; такі запобіжні заходи можуть бути результатом відповідних умов контракту.
14. Установи та органи Спільноти мають інформувати європейського інспектора із захисту даних щодо категорій випадків, коли вони застосовували параграфи 6 та 7.

РОЗДІЛ 3

**СПЕЦІАЛЬНІ КАТЕГОРІЇ ОБРОБКИ ДАНИХ**

*Стаття 10*

# Обробка спеціальних категорій даних

1. Заборонена обробка персональних даних, що розкривають расову чи етнічну приналежність, релігійні або філософські вірування, професійну приналежність, та даних, що стосуються здоров’я або інтимного життя.
2. Параграф 1 не застосовується у наступних випадках:
3. суб’єкт даних надав/надала свою згоду на обробку таких даних, окрім випадків, коли внутрішні правила установи або органу Спільноти встановлюють, що заборона, установлена у параграфі 1 не може бути знята згодою суб’єкту даних, або
4. обробка необхідна для цілей досягнення відповідності особливим правам та зобов’язанням контролера у сфері трудового закону, оскільки це пояснюється в Договорах про заснування Європейських Спільнот або у інших законодавчих інструментах, прийнятих на основі цього, або, якщо необхідно, як узгоджено з європейським інспектором із захисту даних, що підлягає певних заходам безпеки, або
5. обробка даних необхідна для захисту життєво важливих інтересів суб’єкту даних або іншої особи, коли суб’єкт даних фізично або юридично не може надати свою згоду, або
6. обробка стосується даних, які робляться публічними суб’єктом даних для встановлення, виконання або захисту юридичних прав, або
7. обробка проводиться у руслі юридичної діяльності з відповідними заходами безпеки некомерційною організацією, яка є частиною установи або органом Спільноти, не підпорядковується національним законам з захисту даних в силу Статті 4 Директиви 95/46/ЄС, та з політичними, філософськими, релігійними або профспілковим цілями, та за умови, що обробка даних стосується лише членів цієї установи або осіб, які мають з нею постійний контакт стосовно її цілей, та що дані не відкриваються третій стороні без згоди суб’єктів даних.
8. Параграф 1 не застосовується, коли обробка даних є необхідною для цілей превентивної медицини, медичних діагнозів, надання лікування або управління послугами надання медичної допомоги, та коли ці дані обробляються суб’єктом, що працює у медичній сфері, та пов’язаний з професійною таємницею або іншою особою, що також підпорядковується еквівалентній професійній таємниці.
9. Предмет для проведення відповідних засобів безпеки, та з причин суттєвої зацікавленості, виключення на додаток до викладених у параграфі 2, можуть бути викладені в Договорах про заснування Європейських Спільнот або інших законодавчих інструментах, прийнятих на основі цього, або, якщо необхідно, рішенням європейського інспектора із захисту даних.
10. Обробка даних, що стосуються порушень, кримінальних обвинувачень або заходів безпеки, може бути проведена тільки у випадку дозволу згідно з Договорами про заснування Європейських Спільнот або іншими юридичними інструментами, прийнятими на основі цього, або якщо необхідно, європейським інспектором із захисту даних, що підлягає відповідним спеціальним заходам безпеки.
11. Європейський інспектор із захисту даних визначає умови, за яких особовий номер та інша ідентифікуюча інформація загального використання може бути оброблена установою або органом Спільноти.

РОЗДІЛ 4

**ІНФОРМАЦІЯ, ЩО НАДАЄТЬСЯ СУБ’ЄКТУ ДАНИХ**

*Стаття 11*

# Інформація для подання, де були отримані дані від суб'єкта даних

1. Контролер повинен надати суб’єкту даних, у якого/якої отримує дані стосовно його/її, щонайменше наступну інформацію, окрім тієї, що він/вона вже мають:
2. автентичність контролера;
3. цілі операції обробки даних, для якої призначені ці дані;
4. реципієнти даних або категорії реципієнтів;
5. чи є відповіді на запитання обов’язковими чи добровільними, а також можливі наслідки ненадання відповіді;
6. існування права доступу, та права виправляти, дані, що стосуються його або її;
7. будь-яка додаткова інформація, така як:
   1. юридичне підґрунтя для операції обробки даних, для якої ці дані призначені;
   2. часові межі зберігання даних,
   3. право мати звернення до європейського інспектора із захисту даних у будь-який час,

в такій мірі, в якій необхідна подальша інформація, зважаючи на особливі умови, у яких дані були зібрані, щоб гарантувати чесну обробку у відношенні до суб’єкту даних.

1. Шляхом відхилення від параграфу 1, надання інформації або її частини, окрім інформації описаної у параграфі 1(а), (б) та (г), може бути відстрочене на необхідний час для статистичних цілей. Інформація має бути надана, як тільки перестають існувати причини для утримання інформації.

*Стаття 12*

# Інформація для подання, де дані не були отримані від суб'єкта даних

1. У випадках, коли дані не отримані від суб’єкту даних, під час запису персональних даних, або якщо передбачається відкриття третій стороні, не пізніше першого відкриття даних, контролер має надати суб’єкту даних щонайменше наступну інформацію, окрім випадків, коли він чи вона вже мають цю інформацію:
2. особа контролера;
3. цілі обробки даних;
4. категорії даних;
5. реципієнти або категорії реципієнтів;
6. існування права доступу, та права виправляти, дані, що стосуються його або її;
7. будь-яка додаткова інформація, така як:
   1. правова основа для операції обробки даних, для якої ці дані призначені;
   2. часові межі зберігання даних,
   3. право зв’язатися з європейським інспектором із захисту даних у будь-який час,
   4. походження даних, за виключенням випадків, коли контролер не може відкрити цю інформацію через професійну таємницю,

в такій мірі, в якій необхідна подальша інформація, зважаючи на особливі умови, у яких дані обробляються, щоб гарантувати чесну обробку у відношенні до суб’єкту даних.

1. Параграф 1 не застосовується у випадках, коли надання такої інформації є неможливим або викликатиме непропорційні зусилля або якщо запис чи відкриття чітко викладено законом Спільноти, а саме для обробки зі статистичними цілями або для цілей історичного або наукового дослідження. У таких випадках установа або орган Спільноти має надати відповідні заходи безпеки після проведення консультацій з європейським інспектором із захисту даних.

РОЗДІЛ 5

**ПРАВА СУБ’ЄКТУ ДАНИХ**

*Стаття 13*

# Право доступу

Суб’єкт даних має мати право отримувати від контролера, без обмежень, у будь-який час протягом 3 місяців з моменту отримання запиту та безкоштовно:

1. підтвердження стосовно того, чи обробляються дані, що стосуються його або неї;
2. принаймні інформацію стосовно цілей обробки даних, категорій даних, що розглядаються, та реципієнтів або категорій реципієнтів, яким відкриваються дані;
3. інформування у зрозумілій формі стосовно даних, що проходять обробку, та стосовно будь-якої інформації щодо їх джерел;
4. відомості щодо програмування, що застосовується при автоматичній обробці даних, що стосуються його або неї.

*Стаття 14*

# Виправлення

Суб’єкт даних має право на отримання від контролера виправлення без затримки неточних або неповних персональних даних.

*Стаття 15*

# Блокування

1. Суб’єкт даних має право на отримання від контролера блокування даних, коли:
2. їх точність ставиться під питання суб’єктом даних, на період, поки контролер перевірить їх точність, включаючи завершеність даних, або;
3. контролер не потребує їх для завершення своїх завдань, але вони мають зберігатися як докази, або;
4. обробка є незаконною, а суб’єкт даних проти їх знищення і вимагає їх блокування.
5. У автоматичних інформаційних системах, блокування, в принципі, забезпечується технічними засобами. Факт блокування персональних даних буде зазначений у системі таким чином, що відразу стає зрозумілим, що ці персональні дані використовувати не можна.
6. Персональні дані, заблоковані згідно з цією Статтею, будуть, за виключенням зберігання, оброблені для підтвердження, або за умови згоди суб’єкту даних, або для захисту прав третьої сторони.
7. Суб’єкт даних, який запросив і отримав блокування його чи її даних, буде проінформований контролером перед тим, як дані будуть розблоковані.

*Стаття 16*

# Знищення

Суб’єкт даних має право запросити у контролера знищити дані, якщо вони обробляються незаконно, а саме у випадках, коли порушені положення Розділів 1, 2 та 3 Глави ІІ.

*Стаття 17*

# Повідомлення третіх сторін

Суб’єкт даних має право отримати від контролера повідомлення третіх сторін, яким відкриваються дані, щодо виправлень, знищення або блокування згідно зі Статтями 13-16, окрім випадків, коли це є неможливим або вимагає непропорційних зусиль.

*Стаття 18*

# Право суб’єкту даних на заперечення

Суб’єкт даних має право:

1. у будь-який момент часу заперечувати, звертаючись до юридичних підстав, що відносяться до його чи її конкретної ситуації, обробку даних, що стосуються його або її, окрім випадків, вказаних у Статті 5 (б), (в) та (г). У випадках, коли заперечення є обґрунтованим, така обробка не може більше залучати ці дані;
2. бути проінформованим перед тим, як персональні дані розкриваються третій стороні, або перед тим коли вони використовуються від їх імені з цілями прямого маркетингу, а також чітко отримати пропозицію на право безкоштовно заперечити таке розкриття або використання.

*Стаття 19*

# Автоматичні одноосібні рішення

Суб’єкт даних має право не бути предметом рішення, яке викликає юридичні ефекти у відношенні до нього або неї, або суттєво впливає на нього/неї, або який повністю базується на обробці даних, які спрямовані на оцінку певних персональних аспектів, що стосуються його або неї, такі як його/її виконання роботи, надійність або поведінка, окрім випадків, коли таке рішення чітко авторизоване внаслідок національних законів або законів Спільноти, або, якщо необхідно, європейським інспектором із захисту даних. У будь-якому випадку, повинні бути прийняті міри з захисту юридичних інтересів суб’єкту даних, такі як угоди, що дозволяють йому або їй висловити свою думку.

РОЗДІЛ 6

**ВИЛУЧЕННЯ ТА ОБМЕЖЕННЯ**

*Стаття 20*

# Вилучення та обмеження

1. Установи та органи Спільноти можуть обмежити застосування Статті 4(1), Статті 11, Статті 12 (1), Статей 13 до 17 та Статті 37 (1), коли такі обмеження складають міри для забезпечення:
2. запобігання, розслідування, визначення та переслідування кримінальних правопорушень;
3. важливих економічних або фінансових інтересів держави-члена або Європейських Спільнот, включаючи валютні, бюджетні питання, або питання оподаткування;
4. захисту суб’єкту даних або прав і свобод інших осіб;
5. національної безпеки, громадської безпеки або захисту держав-членів;
6. моніторингу, перевірки або регулюючих завдань, пов’язаних, навіть іноді, з роботою офіційних органів у випадках, описаних у (а) та (б).
7. Статті з 13 до 16 не застосовуються у випадках, коли дані обробляються лише з цілями наукового дослідження, або зберігаються у особистій формі протягом часу, що не перевищує період часу необхідний для єдиної цілі збору статистики, за умови, що не існує риску порушення приватності суб’єкту даних, а також що контролер забезпечує відповідні законні гарантії, а саме для забезпечення того, щоб дані не використовувалися для прийняття мір або рішень стосовно певних осіб.
8. Якщо накладається обмеження, вказане у параграфі 1, суб’єкт даних отримує інформацію, згідно з законодавством Спільноти, стосовно головних причин, з яких застосовується таке обмеження, а також його або її право звернутися до європейського інспектора із захисту даних.
9. Якщо обмеження, викладене у параграфі 1 виходить з необхідності закрити доступ до суб’єкту даних, європейський інспектор з захисту даних під час розглядання скарги має лише повідомити його або її стосовно того, чи правильно були оброблені дані, і якщо ні, чи були зроблені необхідні виправлення.
10. Надання інформації, описаної у параграфах 3 та 4 може бути відстроченим настільки, наскільки така інформація знімає обмеження, встановлені параграфом 1.

РОЗДІЛ 7

**КОНФІДЕНЦІЙНІСТЬ ТА БЕЗПЕКА ОБРОБКИ**

*Стаття 21*

# Конфіденційність обробки

Особа, яка працює в установі або органі Спільноти, або установа або орган Спільноти, які виконують роль обробника, з доступом до персональних даних, не можуть їх обробляти, за виключенням випадків, коли надаються інструкції від контролера, якщо це не вимагається національним або законодавством Спільноти.

*Стаття 22*

# Захист обробки

1. Зважаючи на стан технологій та вартість їх імплементації, контролер має впроваджувати доречні технічні та організаційні заходи для забезпечення рівня захисту, що відповідає рівню ризиків, представленим обробкою та природою персональних даних, що мають бути захищеними.

Такі заходи мають вживатися для попередження будь-якого неавторизованого розкриття або доступу, випадкового або незаконного знищення або випадкової втрати, або зміни, а також для попередження усіх інших незаконних форм обробки.

1. У випадках, коли персональні дані обробляються автоматичними засобами, заходи, що приймаються, мають відповідати ризикам, а саме бути спрямованими на:
2. запобігання наданню доступу до комп’ютерних систем, що оброблять персональні дані, неавторизованим особам;
3. запобігання неавторизованому читанню, копіюванню, змінюванню або видаленню даних, що зберігаються;
4. запобігання будь-якому неавторизованому додаванню даних, а також неавторизованому розповсюдженню, внесенню змін або видаленню персональних даних, що зберігаються;
5. запобігання використанню систем обробки даних неавторизованими особами за допомогою засобів передачі даних;
6. забезпечення того, що авторизовані користувачі систем обробки даних мають доступ лише до тих персональних даних, що включені до їх прав доступу;
7. записи про те, які персональні дані були повідомлені, коли та кому;
8. забезпечення того, що буде можливим перевірити, які персональні дані були оброблені, коли та ким;
9. забезпечення того, що персональні дані, які обробляються від імені третьої сторони, можуть бути оброблені лише у спосіб, рекомендований підрядною установою або органом;
10. забезпечення того, що протягом повідомлення персональних даних та протягом транспортування носіїв інформації, дані неможливо прочитати, скопіювати або стерти без авторизації;
11. розробки організаційної структури у межах установи або органу таким чином, що вона відповідатиме спеціальним вимогам захисту даних.

*Стаття 23*

# Обробка персональних даних від імені контролерів

1. У випадках, коли обробка проводиться від його імені, контролер обирає обробника, який надає достатні гарантії відносно заходів технічної та організаційної безпеки, які вимагаються Статтею 22, та забезпечує відповідність тим заходам.
2. Проведення процедури обробки обробником відбувається на основі контракту або законодавчого акту, який пов’язує обробника з контролером та зумовлює наступне:
3. обробник має діяти лише згідно з інструкціями контролера;
4. зобов’язання, вказані у Статтях 21 та 22, покладаються також на обробника, якщо відповідно до Статті 16 або Статті 17(3), другого абзацу Директиви 95/46/ЄС обробник вже підпорядковується зобов’язанням, що стосуються конфіденційності та безпеки, викладеним у національному законі однієї із держав-членів.
5. З метою зберігання доказам, частини контракту або законодавчого акту, які стосуються захисту даних та вимоги відносно заходів, що вказані у Статті 22, мають бути надані у письмовій або іншій еквівалентній формі.

РОЗДІЛ 8

**СПЕЦІАЛІСТ ІЗ ЗАХИСТУ ДАНИХ**

*Стаття 24*

# Призначення та завдання спеціаліста із захисту даних

1. Кожна установа та орган Спільноти мають призначити щонайменше одну особу на посаду спеціаліста із захисту даних. Завдання цієї особи полягає у:
2. забезпеченні інформування контролерів та суб’єктів даних стосовно їх прав та зобов’язань, згідно з даним Регламентом;
3. наданні відповідей на запити від європейського інспектора із захисту даних, та у межах його або її компетенції, співпраці з європейським інспектором із захисту даних по запиту останнього або з його або її власної ініціативи;
4. забезпеченні незалежного внутрішнього застосуванні цього Регламенту;
5. веденні реєстру процедур обробки даних, що проводяться контролером, куди включені елементи інформації, описані у Статті 25(2);
6. повідомленні європейському інспектору із захисту даних про процедури обробки, які можуть спричинити певні ризики у межах Статті 27.

Таким чином, ця особа забезпечує, що процедури обробки даних не спричинять негативного впливу на права та свободи суб’єктів даних.

1. Спеціаліст із захисту даних має обиратися на основі його або її персональних та професійних якостей, і поміж іншого, його або її експертних знаннях у сфері захисту даних.
2. Обрання на посаду спеціаліста із захисту даних не має призвести до конфлікту інтересів між його або її обов’язками як спеціаліста із захисту даних та іншими посадовими обов’язками, а саме у відношенні застосування положень даного Регламенту.
3. Спеціаліст із захисту даних призначається на період від двох до п’яти років. Він або вона можуть знову бути призначеними на цю посаду, але максимальний термін не може перевищувати десяти років. Він або вона можуть бути звільнені з посади спеціаліста із захисту даних установою або органом Спільноти, яка призначила його або її, за згодою з європейським інспектором із захисту даних, якщо він або вона не відповідають умовам, які є необхідними для виконання його або її обов’язків.
4. Після його або її призначення, спеціаліст із захисту даних проходить реєстрацію у європейського інспектора із захисту даних, установою або органом, який його або її призначив.
5. Установа або орган Спільноти, яка призначила спеціаліста із захисту даних, надає йому або їй персонал та ресурси, необхідні для виконання його або її обов’язків.
6. Що стосується виконання його або її обов’язків, спеціаліст із захисту даних може не отримувати ніяких інструкцій.
7. Подальша імплементація правил стосовно спеціаліста із захисту даних проводиться кожною установою або органом Спільноти згідно з положеннями, представленими у Додатку. Правила, що імплементуються мають стосуватися, поміж іншого, завдань, обов’язків та повноважень спеціаліста із захисту даних.

*Стаття 25*

# Повідомлення спеціаліста із захисту даних

1. Контролер має надати попереднє повідомлення спеціалісту із захисту даних стосовно будь-яких процедур обробки даних або наборів таких процедур, що спрямовані на реалізацію однієї цілі або кількох пов’язаних цілей.
2. Інформація, що надається, має включати:
3. ім’я та адресу контролера та ознаку організаційних частин установи або органу, що отримав право на обробку персональних даних з конкретними цілями;
4. ціль або цілі обробки;
5. опис категорії або категорій суб’єктів даних та даних або категорій даних, що до них відносяться;
6. юридичне підґрунтя для операції обробки даних, для якої ці дані призначені;
7. реципієнтів або категорій реципієнтів, яким можуть бути відкриті дані;
8. загальні характеристики часових меж для блокування та знищення різних категорій даних;
9. запропоновану передачу даних третім країнам або міжнародним організаціям;
10. загальний опис, що дозволяє провести попередню оцінку доречності прийнятих засобів згідно за Статтею 22 для забезпечення безпеки обробки.
11. Будь-які зміни, що впливають на інформацію, описану у параграфі 2, мають негайно бути повідомлені спеціалісту із захисту даних.

*Стаття 26*

# Реєстр

Реєстр процедур обробки, повідомлений згідно зі Статтею 25, має зберігатися у кожного спеціаліста із захисту даних.

Реєстри мають містити, принаймні, інформацію, описану у Статті 25(2) (а) до (ж). Реєстри можуть бути перевірені будь-якою особою прямо або опосередковано через європейського інспектора з обробки даних.

РОЗДІЛ 9

**ПОПЕРЕДНЯ ПЕРЕВІРКА ЄВРОПЕЙСЬКИМ ІНСПЕКТОРОМ ІЗ ЗАХИСТУ ДАНИХ ТА ЗОБОВ’ЯЗАННЯ СПІВПРАЦЮВАТИ**

*Стаття 27*

# Попередня перевірка

1. Процедури обробки, які за своєю природою, обсягом та цілями можуть спричинити певні ризики правам та свободам суб’єктів даних, мають підлягати попередній перевірці європейським інспектором із захисту даних.
2. Наступні процедури обробки можуть спричинити такі ризики:
3. обробка даних, що стосуються здоров’я та можливих правопорушень, правопорушень, кримінальних обвинувачень або заходів безпеки;
4. процедури обробки даних, що спрямовані на оцінку особистих аспектів. що стосуються суб’єкту даних, включаючи його або її здатності, ефективність та поведінку;
5. процедури обробки даних, які дозволяють зв’язки між даними, що обробляються з різними цілями, що не відповідає національному законодавству або законодавству Спільноти;
6. процедури обробки з цілями, що позбавляють особи прав, привілеїв або контрактів.
7. Попередні перевірки мають проводитися європейським інспектором із захисту даних, що слідує за повідомленням від відповідальної особи із захисту даних, який, у випадку наявності сумнівів щодо необхідності попередньої перевірки, має звернутися до європейського інспектора із захисту даних.
8. Європейський інспектор із захисту даних має надати його або її думку протягом двох місяців з моменту отримання повідомлення. Цей період може бути подовжений до того часу, коли європейський інспектор із захисту даних отримає будь-яку додаткову інформацію, яку він або вона запросили. Якщо складність питання вимагає, цей період може бути подовжений ще на два місяці, за рішенням європейського інспектора із захисту даних. Це рішення має бути повідомлене контролеру до завершення початкового двомісячного періоду.

Якщо думка не надається до кінця двомісячного періоду, або не повідомляється про подовження періоду, вона вважається схвальною.

Якщо думка європейського інспектора із захисту даних вказує, що зазначена обробка даних може включати порушення будь-яких положень цього Регламенту, він або вона надають пропозиції щодо уникнення таких порушень, де можливо. У випадках, якщо контролер не вносить заміни до процедури обробки згідно з рекомендаціями, європейський інспектор із захисту даних може застосувати повноваження, надані йому або їй згідно зі Статтею 47(1).

1. Європейський інспектор із захисту даних реєструє усі процедури обробки, які були надані йому або їй, згідно з параграфом 2. Реєстр має містити інформацію, вказану в Статті 25, та бути доступним для суспільного контролю.

*Стаття 28*

# Консультація

1. Установи та органи Спільноти мають інформувати європейського інспектора із захисту даних у випадках, коли приймаються адміністративні заходи, що стосуються обробки персональних даних, що включають установу або орган Спільноти окремо або разом з іншими.
2. При прийнятті законодавчої пропозиції, що стосується захисту прав і свобод особистості, зважаючи на обробку персональних даних, Комісія має звернутися до європейського інспектора із захисту даних.

*Стаття 29*

# Зобов’язання надавати інформацію

Установи та органи Спільноти мають інформувати європейського інспектора із захисту даних стосовно заходів, що надалі застосовуються згідно з його або її рішенням або дозволу, як описано у Статті 46 (з).

*Стаття 30*

# Зобов’язання співпрацювати

Згідно з його або її запитом, контролери мають допомагати європейському інспектору із захисту даних у виконанні його або її обов’язків, а саме через надання інформації, яка описана у Статті 47(2)(а) та наданням доступу, як вказано у Статті 47(2)(б).

*Стаття 31*

# Зобов’язання реагувати на заяви

У відповідь на виконання європейським інспектором із захисту даних його або її обов’язків, згідно зі Статтею 47(1)(б), зацікавлений контролер має проінформувати інспектора стосовно своїх поглядів протягом припустимого періоду, що визначається інспектором. Відповідь має також містити опис прийнятих заходів, якщо вони мали місце, у відповідь на зауваження європейського інспектора із захисту даних.

ГЛАВА ІІІ

# ЗАСОБИ СУДОВОГО ЗАХИСТУ

*Стаття 32*

# Засоби судового захисту

1. Суд Європейських Спільнот має юридичне право проводити слухання усіх спірних питань, які стосуються положень цього Регламенту, включаючи позови за нанесені збитки.
2. Без упередженості будь-яких засобів судового захисту, кожний суб’єкт даних може надати скаргу європейському інспектору із захисту даних, якщо він або вона вважає. що його або її права, надані Статтею 286 Договору, були порушені у результаті обробки його або її персональних даних установою або органом Спільноти.

У випадку відсутності відповіді від європейського інспектора із захисту даних протягом шести місяців, скарга вважається відхиленою.

1. Дії, прийняті проти рішень європейського інспектора із захисту даних, будуть передані у Суд Європейських Спільнот.
2. Будь-яка особа, яка постраждала через незаконні процедури обробки даних або будь-які дії, які не відповідають цьому Регламенту, має право на відшкодування збитків згідно зі Статтею 288 Договору.

*Стаття 33*

# Скарги персоналу Спільноти

Будь-яка особа, яка працює в установі або органі Спільноти, може подати скаргу європейському інспектору із захисту даних стосовно можливого порушення положень цього Регламенту, що визначає обробку персональних даних, без надання через офіційні канали. Ніхто не постраждає через надання скарги європейському інспектору із захисту даних, в якій вказується можливе порушення положень, що регулюють обробку персональних даних.

ГЛАВА IV

# ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА ПРИВАТНОСТІ У КОНТЕКСТІ ВНУТРІШНІХ ТЕЛЕКОМУННІКАЦІЙНИХ МЕРЕЖ

*Стаття 34*

# Сфера застосування

Без обмежень інших положень цього Регламенту, ця Глава застосовується до обробки персональних даних у поєднанні з телекомунікаційними мережами або термінальним обладнанням, які працюють під контролем установи або органу Спільноти.

Для цілей цієї Глави, "користувач" означає будь-яку фізичну особу, яка користується телекомунікаційною мережею або термінальним обладнанням, що працює під контролем установи або органу Спільноти.

*Стаття 35*

# Безпека

1. Установи та органи Спільноти мають приймати доречні технічні та організаційні заходи для забезпечення безпеки використання телекомунікаційних мереж та термінального обладнання, якщо це необхідно у поєднанні з провайдерами публічно доступних телекомунікаційних послуг або провайдерами публічних телекомунікаційних мереж. Зважаючи на стан технологій та вартість їх імплементації, ці заходи забезпечують рівень захисту, доречний для представленого ризику.
2. У випадку певного ризику порушення безпеки мережі або термінального обладнання, установа або орган Спільноти мають інформувати користувачів щодо існування такого ризику та можливих заходів його ліквідації та альтернативних засобів комунікації.

*Стаття 36*

# Конфіденційність комунікацій

Установи та органи Спільноти забезпечують конфіденційність комунікацій через телекомунікаційні мережі та термінальне обладнання згідно з загальними принципами законодавства Спільноти.

*Стаття 37*

# Інформація про трафік та білінгові дані

1. Без шкоди для положень параграфів 2, 3 та 4 інформація про трафік користувачів, яка обробляється та зберігається для встановлення дзвінків та інших типів з’єднання через телекомунікаційні мережі має бути знищена або зроблена анонімною після завершення дзвінка або іншого з’єднання.
2. Якщо необхідно, інформація про трафік, як вказано у переліку, узгодженому з європейським інспектором із захисту даних, може бути оброблена для цілей управління телекомунікаційним бюджетом та трафіком, включаючи підтвердження авторизованого використання телекомунікаційних систем. Ця інформація має бути знищена або зроблена анонімною якнайшвидше, але не пізніше ніж через шість місяців після збору, якщо не існує необхідності зберігати ці дані довше для встановлення, виконання або захисту права у юридичному позові, що перебуває у судовому розгляді.
3. Обробка інформації про трафік та білінгових даних має проводитися лише особами, які займаються менеджментом білінгу, трафіку або бюджету.
4. Користувачі телекомунікаційних мереж мають право отримувати перераховані по пунктам рахунки або інші записи, зроблених дзвінків.

*Стаття 38*

# Директорії користувачів

1. Персональні дані, які містяться у роздрукованих або електронних директоріях користувачів та доступ до таких директорій має бути обмежений до того, що є цілком необхідним, для певних цілей директорії.
2. Установи та органи Спільноти приймають необхідні заходи для попередження використання у маркетингових цілях персональних даних, що зберігаються у цих директоріях, незалежно від того, чи знаходяться вони у публічному доступі чи ні.

*Стаття 39*

# Презентація та обмеження ідентифікації дзвінків та лінії з’єднання

1. Якщо пропонується презентація ідентифікації лінії дзвінка, користувач, який дзвонить, має можливість відключити презентацію ідентифікації лінії дзвінка простими засобами та безкоштовно.
2. Якщо пропонується презентація ідентифікації лінії дзвінка, користувач, який отримує дзвінок, має можливість відключити презентацію ідентифікації лінії вхідних дзвінків простими засобами та безкоштовно.
3. Якщо пропонується презентація ідентифікації лінії з’єднання, користувач, який отримує дзвінок, має можливість простими засобами та безкоштовно відключити презентацію ідентифікації лінії з’єднання для користувача, який дзвонить.
4. Коли пропонується ідентифікація лінії дзвінка або з’єднання, установи та органи Спільноти мають інформувати користувачів про це та про можливості, описані у параграфах 1, 2 та 3.

*Стаття 40*

# Часткове скасування

Установи та органи Спільноти забезпечують існування прозорих процедур, що керують способами, якими вони можуть відкидати знищення презентації ідентифікації лінії дзвінка:

1. на тимчасовій основі, після заяви від користувача, з запитом відстежувати зловмисні або надокучливі дзвінки;
2. на основі ліній для організацій, що мають справу з екстреними викликами, для відповіді на такі дзвінки.

ГЛАВА V

# НЕЗАЛЕЖНИЙ КОНТРОЛЬНИЙ ОРГАН: ЄВРОПЕЙСЬКИЙ ІНСПЕКТОР ІЗ ЗАХИСТУ ДАНИХ

*Стаття 41*

# Європейський інспектор із захисту даних

1. Незалежний контрольний орган цьому документі називається європейський інспектор із захисту даних.
2. Зважаючи на обробку персональних даних, європейський інспектор із захисту даних відповідає за забезпечення того, що фундаментальні права та свободи фізичних осіб, поміж іншого, їхнє право на приватність, поважаються установами та органами Спільноти.

Європейський інспектор із захисту даних відповідає за моніторинг та забезпечення реалізації положень цього Регламенту та інших актів Спільноти, які стосуються захисту фундаментальних прав та свобод фізичних осіб відносно обробки персональних даних установами або органами Спільноти, та для надання рекомендацій установам та органам Спільноти та суб’єктам даних з питань, які стосуються обробки персональних даних. З цією метою він або вона виконують обов’язки, описані у Статті 46 та реалізують повноваження, надані у Статті 47.

*Стаття 42*

# Призначення

1. Європейський парламент та Рада призначають європейського інспектора із захисту даних на п’ять років, на основі списку, що надається Комісією після публічного запиту кандидатів.

Помічник інспектора призначається згідно з такою самою процедурою та на такий самий термін, помічник допомагає інспектору у виконанні всіх обов’язків останнього та може замістити інспектора, коли останній відсутній або не може виконувати свої обов’язки.

1. Європейський інспектор із захисту даних обирається серед кандидатів, чия незалежність не підлягає сумнівам, і які визнаються такими, що мають досвід та навички, що є необхідними для виконання обов’язків європейського інспектора із захисту даних, наприклад, тому що вони належать або належали до контролюючих органів, описаних у Статті 28 Директиви 95/46/ЄС.
2. Європейський інспектор із захисту даних може бути повторно призначений.
3. Окрім звичайної заміни або смерті, обов’язки європейського інспектора із захисту даних завершуються у випадку заяви про відставку або обов’язкової відставки згідно з параграфом 5.
4. Європейський інспектор із захисту даних може бути звільнений або позбавлений його або її права на пенсію або інші привілеї європейським судом за запитом Європейського парламенту, Ради або Комісії, якщо він або вона не відповідають умовам, необхідним для виконання його або її обов’язків, або якщо він чи вона винні у серйозних порушеннях.
5. У випадку звичайної заміни або добровільної відставки, європейський інспектор із захисту даних залишається на посаді до тих пір, доки не буде знайдена заміна.
6. Статті 12-15 та 18 Протоколу привілеїв та імунітетів Європейських Спільнот також відноситься до європейського інспектору із захисту даних.
7. Параграфи 2-7 застосовуються до помічника інспектора.

*Стаття 43*

# Регламенти та загальні умови, що регулюють виконання обов’язків європейського інспектора із захисту даних, персоналу та фінансові ресурси

1. Європейський парламент, Рада та Комісія визначають за взаємною згодою регламенти та загальні умови, що регулюють виконання обов’язків європейським інспектором із захисту даних, а саме його або її заробітну платню, суми на витрати та інші привілеї замість компенсацій.
2. Бюджетний орган забезпечує європейського інспектора із захисту даних людськими та фінансовими ресурсами для виконання його або її завдань.
3. Бюджет європейського інспектора із захисту даних буде вказаний у окремій частині стосовно бюджету у Секції VIII загального бюджету Європейського союзу.
4. Європейському інспектору із захисту даних допомагає Секретаріат. Офіційні особи та інший персонал Секретаріату назначаються європейським інспектором із захисту даних; ними керує європейський інспектор із захисту даних та вони підпорядковуються лише його або її вказівкам. Їхня кількість визначається щорічно, як частина процедури визначення бюджету.
5. Офіційні особи та персонал Секретаріату європейського інспектора із захисту даних підпорядковуються правилам та регламентам, які застосовуються до офіційних осіб та інших співробітників Європейських Спільнот.
6. У питаннях, які стосуються персоналу Секретаріату, європейський інспектор із захисту даних отримує такий самий статус, що і установи у межах розуміння Статті 1 Регламентів по персоналу офіційних установ Європейських Спільнот.

*Стаття 44*

# Незалежність

1. Європейський інспектор із захисту даних діє повністю незалежно у виконанні її або його обов’язків.
2. Виконуючи свої обов’язки європейський інспектор із захисту даних не шукає і не виконує інструкції від будь-кого.
3. Європейський інспектор із захисту даних утримується від будь-яких дій, несумісних з його або її обов’язками, а також протягом своєї роботи не приймає участі в інших видах діяльності, незалежно прибуткових чи ні.
4. Після завершення терміну служби європейський інспектор із захисту даних поводиться чесно та обережно при виборі призначень та привілеїв.

*Стаття 45*

# Професійна таємниця

Під час служби та після її завершення європейський інспектор із захисту даних та його або її персонал підпорядковуються обов’язку професійної таємниці, відносно будь-якої конфіденційної інформації, яку вони дізналися протягом виконання своїх посадових обов’язків.

*Стаття 46*

# Обов’язки

Європейський інспектор з захисту даних має:

1. вислуховувати та розслідувати скарги, а також інформувати суб’єкт даних стосовно результатів протягом прийнятного періоду;
2. проводити розслідування чи з власної ініціативи чи на основі скарги, та інформувати суб’єкти даних стосовно результатів у прийнятний період;
3. контролювати та забезпечувати застосування положень цього Регламенту та інших актів Спільноти, які стосуються захисту фізичних осіб відносно обробки персональних даних установами або органами Спільноти за виключенням Суду Європейських Спільнот, який працює у межах своєї юрисдикції;
4. рекомендувати установам та органам Спільноти, з власної ініціативи або у вигляді відповіді на консультацію, стосовно питань, які стосуються обробки персональних даних, а саме до визначення внутрішніх правил, які відносяться до захисту фундаментальних прав та свобод у відношенні обробки персональних даних;
5. проводити моніторинг відповідних розробок, в такій мірі, в якій вони впливають на захист персональних даних, а саме розробок інформаційних та комунікаційних технологій;
6. (і) співпрацювати з національними контролюючими органами, описаними у Статті 28 Директиви 95/46/ЄС у країнах, яких ця Директива стосується у мірі, необхідній для виконання відповідних обов’язків, а саме обміну корисною інформацією, запитувати таку установу або заклад для виконання реалізації своїх повноважень або відреагувати на запит від такої установи або органу;

(іі) також співпрацювати з органами контролю за захистом даних, встановленими у Частині VI Договору Європейського Союзу, а саме намагаючись покращити послідовність при застосуванні правил та процедур, за відповідність яких вони несуть відповідальність;

1. приймати участь у діяльності Робочої групи із захисту особистостей з точки зору обробки персональних даних, створеної Статтею 29 Директиви 95/46/ЄС;
2. визначати, пояснювати причини, опубліковувати виключення, гарантії, авторизації та умови, викладені у Статті 10 (2)(б), (4), (5) та (6), у Статті 12(2), у Статті 19 та Статті 37(2);
3. вести реєстр процедур обробки даних, про які йому або її повідомили відповідно зі Статтею 27(2), та які зареєстровані згідно зі Статтею 27(5), та надавати засоби доступу до реєстрів, які зберігаються у інспекторів із захисту даних згідно зі Статтею 26;
4. проводити попередню перевірку обробки, про яку його або її повідомили;
5. встановлювати його або її правила процедури.

*Стаття 47*

# Повноваження

1. Європейський інспектор із захисту даних може:
2. надавати поради суб’єктам даних стосовно реалізації їх прав;
3. передавати контролеру випадки зареєстрованого порушення положень, які регулюють обробку персональних даних, та коли доцільно, давати поради стосовно виправлення цих порушень та покращення захисту суб’єктів даних;
4. розпоряджатися, щоб запити для виконання певних прав стосовно даних виконувалися, коли такі запити були відхилені через порушення Статей 13-19;
5. попереджувати або застерігати контролера;
6. розпоряджатися про виправлення, блокування, знищення або стирання усіх даних, коли вони були оброблені з порушенням положень, що регулюють обробку персональних даних та повідомляти про такі дії третім сторонам, яким ці дані були відкриті;
7. накладати тимчасову або постійну заборону на обробку даних;
8. передавати питання установі або органу Спільноти, яких стосується це питання, або у випадку необхідності, Європейському Парламенту, Раді або Комісії;
9. передавати випадок до Суду Європейських Спільнот за умов, представлених в Договорі;
10. приймати участь у діях, представлених на розгляд Суду Європейських Спільнот.
11. Європейський інспектор із захисту даних має повноваження:
12. отримати від контролера або установи чи органу Спільноти доступ до персональних даних та до усієї інформації, необхідної для його чи її розслідування;
13. отримати доступ до будь-якої нерухомості, де контролер або установа або орган Спільноти проводять свою діяльність, коли існують суттєві підстави вважати, що будь-яка діяльність, що підпадає під цей Регламент, проводиться там .

*Стаття 48*

# Звіт про діяльність

1. Європейський інспектор із захисту даних надає щорічний звіт про свою діяльність до Європейського Парламенту, Ради та Комісії, в той самий час оприлюднюючи його.
2. Європейський інспектор із захисту даних надає звіт про діяльність іншим установам та органам Спільноти, які можуть внести коментарі з точки зору можливої перевірки звіту у Європейському Парламенті, а саме у відношенні опису заходів, прийнятих у відповідь на коментарі, зроблені європейським інспектором із захисту даних згідно зі Статтею 31.

ГЛАВА VI

# КІНЦЕВІ ПОЛОЖЕННЯ

*Стаття 49*

# Санкції

Нездатність виконувати зобов’язання, що витікають з цього Регламенту, навмисно чи через недбалість з його або її сторони, робить інспектора або іншого службовця Європейських Спільнот підпорядкованим дисциплінарним діям, згідно з правилами та процедурами, викладеними у Регламенті щодо персоналу офіційних установ Європейських Спільнот або умовами роботи, що застосовуються до інших службовців.

*Стаття 50*

# Перехідний період

Установи та органи Спільноти гарантують, що обробка даних, яка має місце на момент, коли цей Регламент набуде чинності, будуть приведені до відповідності з цим Регламентом протягом одного року з дати набуття чинності.

*Стаття 51*

# Набуття чинності

Цей Регламент набуває чинності на двадцятий день після публікації у *Офіційному віснику Європейських Спільнот*.

Цей Регламент повністю використовується та прямо застосовується в усіх державах-членах. Підписаний у Брюсселі, 18 грудня 2000 року.

*Для Європейського Парламенту Президент*

N. FONTAINE

*Для Ради Президент*

D. VOYNET



*ДОДАТОК*

1. Європейський інспектор із захисту даних може надавати рекомендації стосовно практичного покращення захисту даних установам та органам Спільноти, які призначили його або її, а також давати поради їм та контролеру стосовно питань щодо реалізації положень захисту даних. Крім того, він або вона, за власної ініціативи або за запитом від установи чи органу, які призначили його або її, контролера, Комітету з персоналу, або будь-якої особи, розслідувати питання та випадки, які безпосередньо пов’язані з його або її завданнями, та які потрапляють в його або її поле зору, та звітуватися особі, яка доручила розслідування або контролеру.
2. Установа або орган Спільноти, які призначили європейського інспектора із захисту даних, зацікавлений контролер, зацікавлений Комітет з персоналу або будь-яка особа можуть звертатися до європейського інспектора із захисту даних без офіційних каналів з будь-яких питань, які стосуються інтерпретації або застосування даного Регламенту.
3. Ніхто не має страждати від упереджень стосовно питань, на які звернули увагу компетентного інспектора із захисту даних, заявляючи, що мало місце порушення положень цього Регламенту.
4. Кожний зацікавлений контролер має допомагати інспектору із захисту даних у виконанні останнім своїх обов’язків та надавати інформацію у відповідь на запитання. При виконанні своїх обов’язків, інспектор із захисту даних має мати доступ у будь-який час до даних, які формують предмет дослідження процедур дослідження даних, а також до усіх офісів, обладнання обробки даних та носіїв даних.
5. В необхідній мірі інспектор із захисту даних звільняється від іншої діяльності. Інспектор із захисту даних та його або її персонал, до яких застосовується Стаття 287 Договору, не мають права розголошувати інформацію та оприлюднювати інформацію, які вони отримують при виконанні своїх обов’язків.

