# РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) № 910/2014

## від 23 липня 2014 року

## про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ І РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про функціонування Європейського Союзу, зокрема його статтю 114,

Беручи до уваги пропозицію Європейської Комісії,

Після передачі проекту законодавчого акта національним парламентам,

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

Діючи згідно зі звичайною законодавчою процедурою ([2]),

Оскільки:

(1) Побудова довіри в онлайн-середовищі є ключовою для економічного та соціального розвитку. Через брак довіри, зокрема внаслідок відчутного браку правової визначеності, споживачі, суб'єкти підприємницької діяльності, а також органи публічної влади вагаються здійснювати транзакції в електронній формі та впроваджувати нові послуги.

(2) Цей Регламент має на мені підвищити рівень довіри до електронних транзакцій на внутрішньому ринку шляхом створення спільного підґрунтя для безпечної електронної взаємодії між громадянами, суб'єктами підприємницької діяльності та органами публічної влади, покращуючи у такий спосіб дієвість публічних і приватних онлайн-послуг, електронного бізнесу та електронної комерції в Союзі.

(3) Директива Європейського Парламенту і Ради 1999/93/ЄС ([3]) регулювала питання електронних підписів без встановлення всебічних транскордонних та міжсекторальних рамок для безпечних, надійних і простих у використанні електронних транзакцій. Цей Регламент удосконалює та розширює acquis зазначеної Директиви.

(4) У повідомленні Комісії під назвою «Цифровий порядок денний Європи» від 26 серпня 2010 року визначено фрагментацію цифрового ринку, брак інтероперабельності та зростання кіберзлочинності основними перешкодами для успішного циклу розвитку цифрової економіки. У своєму Звіті про громадянство ЄС 2010 року під назвою «Ліквідація перешкод для реалізації прав громадян ЄС» Комісія додатково наголосила на необхідності вирішення основних проблем, які перешкоджають громадянам Союзу користуватися перевагами єдиного цифрового ринку і транскордонних цифрових послуг.

(5) У своїх висновках від 4 лютого 2011 року та 23 жовтня 2011 року Європейська Рада запропонувала Комісії створити до 2015 року єдиний цифровий ринок, досягнути швидкого прогресу в ключових сферах цифрової економіки та сприяти повністю інтегрованому єдиному цифровому ринку шляхом спрощення транскордонного використання онлайн-послуг, приділяючи особливу увагу спрощенню безпечної електронної ідентифікації та автентифікації.

(6) У своїх висновках від 27 травня 2011 року Рада запропонувала Комісії зробити внесок у розвиток єдиного цифрового ринку шляхом створення належних умов для взаємного транскордонного визнання таких ключових супутніх чинників, як електронна ідентифікація, електронні документи, електронні підписи та реєстрованої електронної доставки, та для надання інтероперабельних послуг електронного врядування на всій території Європейського Союзу.

(7) У своїй резолюції від 21 вересня 2010 року про завершення формування внутрішнього ринку для електронної комерції ([4]) Європейський Парламент підкреслив важливість безпеки електронних послуг, зокрема електронних підписів, та необхідність створення інфраструктури відкритих ключів на пан'європейському рівні, і закликав Комісію створити портал європейських органів валідації для

# РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) № 910/2014

## від 23 липня 2014 року

## про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ І РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

Беручи до уваги Договір про функціонування Європейського Союзу, зокрема його статтю 114,

Беручи до уваги пропозицію Європейської Комісії,

Після передачі проекту законодавчого акта національним парламентам,

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

Діючи згідно зі звичайною законодавчою процедурою [2],

Оскільки:

(1) Побудова довіри в онлайн-середовищі є ключовою для економічного та соціального розвитку. Через брак довіри, зокрема внаслідок відчутного браку правової визначеності, споживачі, суб'єкти підприємницької діяльності, а також органи публічної влади вагаються здійснювати транзакції в електронній формі та впроваджувати нові послуги.

(2) Цей Регламент має на мені підвищити рівень довіри до електронних транзакцій на внутрішньому ринку шляхом створення спільного підґрунтя для безпечної електронної взаємодії між громадянами, суб'єктами підприємницької діяльності та органами публічної влади, покращуючи у такий спосіб дієвість публічних і приватних онлайн-послуг, електронного бізнесу та електронної комерції в Союзі.

(3) Директива Європейського Парламенту і Ради 1999/93/ЄС [3] регулювала питання електронних підписів без встановлення всебічних транскордонних та міжсекторальних рамок для безпечних, надійних і простих у використанні електронних транзакцій. Цей Регламент удосконалює та розширює *acquis* зазначеної Директиви.

(4) У повідомленні Комісії під назвою «Цифровий порядок денний Європи» від 26 серпня 2010 року визначено фрагментацію цифрового ринку, брак інтероперабельності та зростання кіберзлочинності основними перешкодами для успішного циклу розвитку цифрової економіки. У своєму Звіті про громадянство ЄС 2010 року під назвою «Ліквідація перешкод для реалізації прав громадян ЄС» Комісія додатково наголосила на необхідності вирішення основних проблем, які перешкоджають громадянам Союзу користуватися перевагами єдиного цифрового ринку і транскордонних цифрових послуг.

(5) У своїх висновках від 4 лютого 2011 року та 23 жовтня 2011 року Європейська Рада запропонувала Комісії створити до 2015 року єдиний цифровий ринок, досягнути швидкого прогресу в ключових сферах цифрової економіки та сприяти повністю інтегрованому єдиному цифровому ринку шляхом спрощення транскордонного використання онлайн-послуг, приділяючи особливу увагу спрощенню безпечної електронної ідентифікації та автентифікації.

(6) У своїх висновках від 27 травня 2011 року Рада запропонувала Комісії зробити внесок у розвиток єдиного цифрового ринку шляхом створення належних умов для взаємного транскордонного визнання таких ключових супутніх чинників, як електронна ідентифікація, електронні документи, електронні підписи та реєстрованої електронної доставки, та для надання інтероперабельних послуг електронного врядування на всій території Європейського Союзу.

(7) У своїй резолюції від 21 вересня 2010 року про завершення формування внутрішнього ринку для електронної комерції [4] Європейський Парламент підкреслив важливість безпеки

електронних послуг, зокрема електронних підписів, та необхідність створення інфраструктури відкритих ключів на пан'європейському рівні, і закликав Комісію створити портал європейських органів валідації для забезпечення транскордонної інтероперабельності електронних підписів та підвищення рівня безпеки транзакцій, що їх проводять з використанням інтернету.

(8) Директива Європейського Парламенту і Ради 2006/123/ЄС [(5)] вимагає від держав-членів встановлення єдиних пунктів зв'язку, щоб забезпечити можливість виконання всіх процедур і формальностей, пов'язаних із доступом до діяльності з надання послуг та їх провадженням, у легкий спосіб, на відстані та за допомогою електронних засобів через відповідний єдиний пункт зв'язку з відповідними органами. Багато онлайн-послуг, доступних через єдиний пункт зв'язку, вимагають електронної ідентифікації, електронної автентифікації та проставлення електронного підпису.

(9) У більшості випадків громадяни не можуть використати свою електронну ідентифікацію для автентифікації своєї особи в іншій державі-члені, оскільки інші держави-члени не визнають національні схеми електронної ідентифікації в країні таких громадян. Така цифрова перешкода не дозволяє надавачам послуг користуватися всіма перевагами внутрішнього ринку. Взаємне визнання засобів електронної ідентифікації полегшить транскордонне надання численних послуг на внутрішньому ринку і надасть змогу суб'єктам підприємницької діяльності функціонувати на транскордонній основі, не наражаючись на численні перешкоди під час взаємодії з органами публічної влади.

(10) У Директиві Європейського Парламенту і Ради 2011/24/ЄС [(6)] встановлено мережу національних органів влади, відповідальних за електронну систему охорони здоров'я. Для покращення безпеки і безперервності транскордонного медичного обслуговування від цієї мережі вимагають розробити настанови щодо транскордонного доступу до електронних даних про стан здоров'я і послуг, у тому числі шляхом підтримання «спільних заходів з ідентифікації та автентифікації для полегшення передання даних у межах транскордонного медичного обслуговування». Взаємне визнання електронної ідентифікації та автентифікації є ключовим елементом для втілення у життя транскордонного медичного обслуговування для громадян Європи. Коли люди подорожують із метою лікування, їхні медичні дані повинні бути доступними в країні лікування. Це вимагає ґрунтовних, безпечних та надійних рамок для електронної ідентифікації.

(11) Цей Регламент необхідно застосовувати у повній відповідності з принципами, пов'язаними із захистом персональних даних і передбаченими у Директиві Європейського Парламенту і Ради 95/46/ЄС [(7)]. У цьому зв'язку, враховуючи встановлений у цьому Регламенті принцип взаємного визнання, автентифікація для онлайн-послуги повинна стосуватися опрацювання лише тих ідентифікаційних даних, які є достатніми, належними та незайвими для надання доступу до такої онлайн-послуги. Крім того, надавачам довірчих послуг та наглядовим органам необхідно дотримуватися передбачених у Директиві 95/46/ЄС вимог до збереження конфіденційності та безпеки опрацювання.

(12) Однією з цілей цього Регламенту є усунення наявних перешкод для транскордонного використання засобів електронної ідентифікації, що їх використовують у державах-членах для автентифікації, щонайменше для публічних послуг. У межах цього Регламенту не мають на меті втручатися у питання щодо систем управління електронними ідентифікаційними даними і пов'язаних інфраструктур, створених на території держав-членів. Мета цього Регламенту полягає у забезпеченні можливості безпечної електронної ідентифікації та автентифікації для доступу до транскордонних онлайн-послуг, що їх пропонують держави-члени.

(13) Держави-члени повинні мати вільну можливість використовувати або впроваджувати засоби електронної ідентифікації для доступу до онлайн-послуг. Вони також повинні мати змогу вирішувати, чи залучати приватний сектор до надання таких засобів. Держави-члени не повинні бути зобов'язані нотифікувати Комісії свої схеми електронної ідентифікації. Держави-члени вирішують, чи нотифікувати Комісії усі схеми електронної ідентифікації, використовувані на національному рівні для доступу щонайменше до публічних онлайн-послуг або конкретних послуг, про деякі з них чи не повідомляти про жодні з них.

(14)У Регламенті повинні бути встановлені певні умови щодо засобів електронної ідентифікації, які необхідно визнати, та способів нотифікації схем електронної ідентифікації. Такі умови повинні допомогти державам-членам побудувати між собою необхідну довіру до схем електронної ідентифікації та взаємно визнати засоби електронної ідентифікації, що перебувають у межах їхніх нотифікованих схем. Необхідно застосовувати принцип взаємного визнання, якщо схема електронної ідентифікації держави-члена, що здійснює нотифікацію, відповідає умовам нотифікації та нотифікацію опубліковано в *Офіційному віснику Європейського Союзу*. Проте принцип взаємного визнання повинен стосуватися лише автентифікації для онлайн-послуги. Доступ до таких онлайн-послуг та їх кінцеве надання замовникові повинні бути тісно пов'язані з правом на отримання таких послуг на умовах, установлених у національному законодавстві.

(15)Обов'язок визнавати засоби електронної ідентифікації повинен стосуватися тільки тих засобів, рівень надійності ідентифікаційних даних для яких рівнозначний рівню, необхідному для відповідної онлайн-послуги, або вищий за нього. Крім того, такий обов'язок необхідно застосовувати тільки тоді, коли відповідний орган публічного сектора використовує рівень надійності «істотний» або «високий» у зв'язку з доступом до такої онлайн-послуги. Відповідно до права Європейського Союзу держави-члени повинні мати вільну можливість визнавати засоби електронної ідентифікації, що мають нижчий рівень надійності ідентифікаційних даних.

(16)Рівні надійності повинні характеризувати ступінь довіри до засобу електронної ідентифікації під час встановлення тотожності особи, запевняючи у такий спосіб, що особа, яка заявляє про певну тотожність, насправді є особою, якій було присвоєно таку тотожність. Рівень надійності залежить від ступеня довіри, який забезпечує засіб електронної ідентифікації для заявленої або ствердженої тотожності особи з урахуванням процесів (наприклад, підтвердження і верифікація тотожності особи та автентифікація), діяльності з управління (наприклад, суб'єкт, що видає засоби електронної ідентифікації, та процедура випуску таких засобів) та впроваджених механізмів технічного контролю. Різні технічні визначення та описи рівнів надійності виникли внаслідок великомасштабних дослідних проектів, які фінансує ЄС, стандартизації та міжнародної діяльності. Зокрема, великомасштабний дослідний проект STORK та стандарт ISO 29115 покликаються, між іншим, на рівні 2, 3 і 4, які необхідно найбільше врахувати під час установлення мінімальних технічних вимог, стандартів та процедур для рівнів надійності «низький», «істотний» та «високий» у розумінні цього Регламенту, забезпечуючи разом з цим узгоджене застосування цього Регламенту, зокрема щодо рівня надійності «високий», пов'язаного з підтвердженням тотожності особи для видання кваліфікованих сертифікатів. Установлені вимоги повинні бути технологічно нейтральними. Слід забезпечити можливість досягнення необхідних вимог до безпеки шляхом використання різних технологій.

(17)Держави-члени повинні заохочувати приватний сектор добровільно використовувати засоби електронної ідентифікації за нотифікованою схемою з метою ідентифікації, коли це є необхідним для онлайн-послуг або електронних транзакцій. Можливість використання таких засобів електронної ідентифікації надасть змогу приватному сектору покладатися на електронну ідентифікацію та автентифікацію, що вже широко використовуються в багатьох державах-членах, щонайменше для публічних послуг та полегшити суб'єктам підприємницької діяльності та громадянам доступ до їхніх транскордонних онлайн-послуг. Для того, щоб сприяти транскордонному використанню приватним сектором таких засобів електронної ідентифікації, надана будь-якою державою-членом можливість автентифікації повинна бути доступною для сторін-користувачів приватного сектора, заснованих за межами держави-члена, на таких самих умовах, як ті, що застосовують до сторін-користувачів приватного сектора, заснованих у межах держави-члена. Відповідно, щодо сторін-користувачів приватного сектора держава-член, що здійснює нотифікацію, може визначити умови доступу до засобів автентифікації. У межах таких умов доступу можуть повідомляти, чи доступні на разі для сторін-користувачів приватного сектора засоби автентифікації, пов'язані з нотифікованою схемою.

(18)У цьому Регламенті необхідно передбачати відповідальність держави-члена, що здійснює нотифікацію, сторони, що випускає засоби електронної ідентифікації, та сторони, що виконує процедуру автентифікації, за невиконання відповідних обов'язків за цим

Регламентом. Проте цей Регламент необхідно застосовувати відповідно до національних правил щодо відповідальності. Тому він не впливає на такі національні правила щодо, зокрема, визначення шкоди, або на застосовні процедурні правила, в тому числі щодо тягаря доказування.

(19) Безпека схем електронної ідентифікації є ключовою для благонадійного транскордонного взаємного визнання засобів електронної ідентифікації. У цьому контексті держави-члени повинні співпрацювати в питаннях безпеки та інтероперабельності схем електронної ідентифікації на рівні Європейського Союзу. Щоразу, коли схеми електронної ідентифікації вимагають специфічного апаратного або програмного забезпечення, яке використовуватимуть сторони-користувачі на національному рівні, транскордонна інтероперабельність передбачає, щоб такі держави-члени не покладали виконання таких вимог і пов'язані з ними витрати на сторін-користувачів, заснованим за межами їхніх територій. У цьому випадку відповідні рішення необхідно обговорювати і розробляти в рамках інтероперабельності. Тим не менш, неминучим є встановлення технічних вимог, які випливають із характерних специфікацій національних засобів електронної ідентифікації та можуть мати вплив на держателів таких електронних засобів (наприклад, смарт-карт).

(20) Співпраця держав-членів повинна сприяти технічній інтероперабельності нотифікованих схем електронної ідентифікації з метою створення високого рівня довіри і безпеки, що відповідає ступеню ризику. Обмін інформацією та найкращими практиками між державами-членами з метою їх взаємного визнання повинен сприяти такій співпраці.

(21) У цьому Регламенті необхідно також встановити загальні правові рамки для використання довірчих послуг. Проте такі рамки не повинні створювати загального обов'язку використовувати їх або встановлювати пункт доступу до всіх наявних довірчих послуг. Зокрема, вони не повинні охоплювати послуги, використовувані винятково визначеною групою учасників у межах закритих систем, які не мають впливу на третіх осіб. Наприклад, системи, створені у суб'єктах підприємницької діяльності або публічних адміністраціях для управління внутрішніми процедурами з використанням довірчих послуг, не повинні підпадати під дію вимог цього Регламенту. Лише довірчі послуги, що їх надають широкому загалу і вплив яких поширюється на третіх осіб, повинні відповідати вимогам, установленим у Регламенті. Цей Регламент також не повинен охоплювати аспекти, пов'язані з укладенням та чинністю договорів або інших юридичних обов'язків, де є вимоги щодо форми, встановленої національним правом або правом Союзу. Крім того, він не повинен впливати на національні вимоги щодо форм, пов'язаних із публічними реєстрами, зокрема комерційними і земельними реєстрами.

(22) Для того, щоб сприяти загальному транскордонному використанню довірчих послуг, повинна існувати можливість використовувати їх як докази в провадженнях в усіх державах-членах. Саме національне право визначає юридичну силу довірчих послуг, якщо інше не передбачено у цьому Регламенті.

(23) Тією мірою, в якій цей Регламент створює обов'язок визнавати довірчу послугу, таку довірчу послугу може бути відхилено лише в тому випадку, коли адресат обов'язку не може прочитати або верифікувати її з технічних причин, що перебувають поза безпосереднім контролем адресата. Проте такий обов'язок не повинен сам по собі вимагати від публічного органу отримання апаратного та програмного забезпечення, необхідного для технічного зчитування всіх наявних довірчих послуг.

(24) Держави-члени можуть підтримувати або впроваджувати національні положення, які відповідають праву Європейського Союзу та пов'язані з довірчими послугами, якщо такі послуги не повною мірою згармонізовано з цим Регламентом. Проте довірчі послуги, які відповідають цьому Регламенту, повинні вільно ширитися у межах внутрішнього ринку.

(25) Окрім тих довірчих послуг, що входять у закритий список довірчих послуг, передбачений у цьому Регламенті, держави-члени повинні мати вільну можливість визначати довірчі послуги інших типів з метою їх визнання на національному рівні як кваліфікованих довірчих послуг.

(26) Враховуючи темп технологічних змін, у межах цього Регламенту необхідно ухвалити підхід, відкритий для інновацій.

(27)Цей Регламент повинен бути технологічно нейтральним. Його правових наслідків необхідно досягти за допомогою будь-яких технічних засобів, що відповідають вимогам цього Регламенту.

(28)Для того, щоб, зокрема, підвищити рівень довіри саме до малих та середніх підприємств і споживачів на внутрішньому ринку та сприяти використанню довірчих послуг і продуктів, необхідно ввести поняття кваліфікованих довірчих послуг та кваліфікованого надавача довірчих послуг з метою зазначення вимог та обов'язків, що забезпечують високий рівень безпеки будь-яких використовуваних або надаваних кваліфікованих довірчих послуг і продуктів.

(29)Відповідно до зобов'язань за Конвенцією Організації Об'єднаних Націй про права осіб з інвалідністю, схваленою Рішенням Ради 2010/48/ЄС (8), зокрема за її статтею 9, особи з інвалідністю повинні мати можливість використовувати довірчі послуги та продукти для кінцевих користувачів, використовувані у межах надання таких послуг, на тій самій основі, що й інші споживачі. Тому, за можливості, надавані довірчі послуги та продукти для кінцевих користувачів, використовувані для надання таких послуг, повинні бути доступними для осіб з інвалідністю. Оцінювання можливості повинно також охоплювати, між іншим, технічні та економічні міркування.

(30)Держави-члени повинні призначити наглядовий орган або наглядові органи для здійснення наглядової діяльності за цим Регламентом. Держави-члени повинні також мати змогу ухвалити рішення, за взаємною домовленістю з іншою державою-членом, про призначення наглядового органу на території такої іншої держави-члена.

(31)Наглядові органи повинні співпрацювати з органами захисту даних, наприклад, інформуючи останніх про результати аудитів кваліфікованих надавачів довірчих послуг, якщо виявлено, що правила захисту персональних даних порушено. Надання інформації повинно, зокрема, охоплювати повідомлення про інциденти порушення безпеки та порушення режиму захисту персональних даних.

(32)На всіх надавачів довірчих послуг необхідно покласти обов'язок застосовувати належну практику безпеки, яка відповідає ризикам, пов'язаним з їхньою діяльністю, щоб підвищити рівень довіри користувачів до єдиного ринку.

(33)Положення про використання псевдонімів у сертифікатах не повинні перешкоджати державам-членам вимагати ідентифікації осіб відповідно до права Союзу або національного права.

(34)Усім державам-членам необхідно дотримуватися спільних суттєвих вимог до нагляду, щоб забезпечити зіставний рівень безпеки кваліфікованих довірчих послуг. Для полегшення узгодженого застосування таких вимог на території Союзу держави-члени повинні ухвалити зіставні процедури та здійснювати обмін інформацією про свою наглядову діяльність та найкращі практики у цій сфері.

(35)Усі надавачі довірчих послуг повинні підпадати під дію вимог цього Регламенту, зокрема вимог до безпеки та відповідальності, щоб забезпечити належну сумлінність, прозорість та підзвітність їхніх операцій та послуг. Однак враховуючи тип послуг, які надають надавачі довірчих послуг, доцільно, коли йдеться про такі вимоги, розрізняти кваліфікованих та некваліфікованих надавачів довірчих послуг.

(36)Установлення наглядового режиму для всіх надавачів довірчих послуг повинно забезпечити рівні умови для безпеки та підзвітності їхніх операцій та послуг, тим самим сприяючи захистові користувачів та функціонуванню внутрішнього ринку. Надавачі кваліфікованих довірчих послуг повинні підпадати під необтяжувальну та реагівну наглядову діяльність *ex post*, що ґрунтується на характері їхніх послуг та операцій. Тому наглядовий орган не повинен мати загального обов'язку здійснювати нагляд за некваліфікованими надавачами послуг. Наглядовий орган повинен вживати заходів у разі повідомлення йому (наприклад, безпосередньо некваліфікованим надавачем довірчих послуг, іншим наглядовим органом, користувачем чи діловим партнером або на підставі свого власного розслідування) про те, що некваліфікований надавач довірчих послуг не виконує вимог цього Регламенту.

(37)У цьому Регламенті необхідно передбачити відповідальність усіх надавачів довірчих послуг.

Зокрема, у ньому встановлюють режим відповідальності, відповідно до якого всі надавачі довірчих послуг повинні нести відповідальність за шкоду, спричинену будь-якій фізичній або юридичній особі через невиконання обов'язків за цим Регламентом. Для того, щоб полегшити проведення оцінювання фінансового ризику, який надавачі довірчих послуг можуть нести або повинні покривати страховими полісами, цей Регламент дає останнім змогу встановлювати, за певних умов, обмеження у використанні надаваних ними послуг та не нести відповідальність за шкоду, спричинену перевищенням таких обмежень у використанні зазначених послуг. Клієнтів необхідно належно поінформувати про обмеження заздалегідь. Ці обмеження повинні стати впізнаваними для третьої особи, наприклад, шляхом включення інформації про обмеження в умови надання послуги або шляхом використання інших впізнаваних засобів. Для цілей введення в дію таких принципів цей Регламент необхідно застосовувати відповідно до національних правил щодо відповідальності. Тому цей Регламент не впливає на такі національні правила щодо, зокрема, визначення шкоди, умислу, необережності, або відповідні застосовні процедурні правила.

(38) Повідомлення про порушення безпеки та оцінювання ризиків порушення безпеки є суттєвими для надання належної інформації відповідним особам у разі порушення безпеки або втрати цілісності.

(39) Для надання можливості Комісії та державам-членам оцінити дієвість механізму повідомлення про порушення, який впроваджують у цьому Регламенті, до наглядових органів необхідно звернутися з проханням про надання підсумкової інформації Комісії та Європейському агентству мережевої та інформаційної безпеки (ENISA).

(40) Для надання можливості Комісії та державам-членам оцінити дієвість удосконаленого механізму нагляду, який впроваджують у цьому Регламенті, до наглядових органів необхідно звернутися з проханням про надання звітів про його діяльність. Це послугувало б спрощенню обміну належною практикою між наглядовими органами та забезпечило б перевірку узгодженої та ефективної реалізації суттєвих вимог до нагляду в усіх державах-членах.

(41) Для того, щоб забезпечити стабільність та довготривалість кваліфікованих довірчих послуг і підвищити рівень довіри користувачів до безперервності надання кваліфікованих довірчих послуг, наглядові органи повинні перевірити наявність і правильне застосування положень щодо планів припинення дії в разі припинення діяльності кваліфікованими надавачами довірчих послуг.

(42) Для того, щоб полегшити нагляд за кваліфікованими надавачами довірчих послуг, наприклад, якщо надавач надає свої послуги на території іншої держави-члена і не підлягає там нагляду або якщо комп'ютери надавача розташовані на території держави-члена, відмінної від тієї, у якій його засновано, необхідно створити систему взаємної допомоги між наглядовими органами в державах-членах.

(43) Для забезпечення відповідності кваліфікованих надавачів довірчих послуг та послуг, які вони надають, викладеним у цьому Регламенті вимогам, органу з оцінювання відповідності необхідно здійснювати оцінювання відповідності, а кваліфікованим надавачам довірчих послуг необхідно надати підсумкові звіти про оцінювання відповідності наглядовому органу. Щоразу, коли наглядовий орган вимагає від кваліфікованого надавача довірчих послуг надати звіт про оцінювання відповідності ad hoc, наглядовий орган повинен дотримуватися, зокрема, принципів належного управління, у тому числі обов'язку обґрунтовувати свої рішення, а також принципу пропорційності. Тому наглядовий орган повинен належно обґрунтувати своє рішення про вимогу проведення оцінювання відповідності ad hoc.

(44) Метою цього Регламенту є забезпечення узгоджених рамок для забезпечення високого рівня безпеки та правової визначеності довірчих послуг. У зв'язку з цим, займаючись оцінюванням відповідності продукції та послуг, Комісія, за доцільності, повинна прагнути досягти ефекту від взаємодії з відповідними чинними європейськими та міжнародними схемами, такими як Регламент Європейського Парламенту і Ради (ЄС) № 765/2008 [(9)], у якому встановлено вимоги до акредитації органів з оцінювання відповідності та ринкового нагляду за продуктами.

(45) З метою забезпечення ефективного процесу ініціювання, який повинен привести до

включення кваліфікованих надавачів довірчих послуг і надаваних ними кваліфікованих довірчих послуг до довірчих списків, слід заохочувати до попередньої співпраці потенційних кваліфікованих надавачів довірчих послуг і компетентних наглядових органів з метою сприяння забезпеченню належної сумлінності, що веде до надання кваліфікованих довірчих послуг.

(46) Довірчі списки є суттєвими елементами у побудові довіри між учасниками ринку, оскільки вони вказують на кваліфікований статус надавача довірчих послуг під час здійснення нагляду.

(47) Довіра до онлайн-послуг і їхня зручність є суттєвими для того, щоб користувачі могли повною мірою скористатися електронними послугами і свідомо розраховувати на них. З цією метою необхідно створити знак довіри ЄС для ідентифікації кваліфікованих довірчих послуг, що їх надають кваліфіковані надавачі довірчих послуг. Такий знак довіри ЄС до кваліфікованих довірчих послуг чітко вирізнятиме кваліфіковані довірчі послуги з-поміж інших довірчих послуг, сприяючи прозорості ринку. Використання знаку довіри ЄС кваліфікованими надавачами довірчих послуг повинно бути добровільним і не повинно призводити до виконання інших вимог, відмінних від передбачених у цьому Регламенті.

(48) Хоча для забезпечення взаємного визнання електронних підписів необхідний високий рівень безпеки, у конкретних випадках, наприклад, у контексті Рішення Комісії 2009/767/ЄС [(10)], електронні підписи з нижчим рівнем безпеки також необхідно приймати.

(49) У цьому Регламенті необхідно встановити принцип, згідно з яким електронний підпис не можна позбавити юридичної сили на підставі його електронної форми або його невідповідності вимогам кваліфікованого електронного підпису. Проте саме у національному праві визначають юридичну силу електронних підписів, за винятком випадків, коли за вимогами, передбаченими у цьому Регламенті кваліфікований електронний підпис повинен мати юридичну силу, рівнозначну власноручному підпису.

(50) Оскільки компетентні органи в державах-членах на даний час використовують різні формати вдосконалених електронних підписів для підписання своїх документів в електронній формі, необхідно забезпечити технічне підтримування принаймні декількох форматів удосконалених електронних підписів у державах-членах, коли вони отримують документи, підписані в електронній формі. Подібним чином, коли компетентні органи в державах-членах використовують удосконалені електронні печатки, було б необхідно забезпечити підтримування ними принаймні декількох форматів удосконалених електронних печаток.

(51) Підписувач повинен мати можливість доручити засоби для створення кваліфікованого електронного підпису третім особам за умови, що буде впроваджено належні механізми та процедури для забезпечення одноосібного контролю підписувача за використанням його даних про створення електронного підпису, та за умови, що використання зазначених засобів відповідає вимогам до кваліфікованого електронного підпису.

(52) Створення віддалених електронних підписів за умови управління середовищем створення електронних підписів надавачем довірчих послуг від імені підписувача потребує розширення у світлі їхніх численних економічних вигод. Проте для того, щоб забезпечити юридичне визнання таких електронних підписів, рівнозначне визнанню електронних підписів, створених у середовищі, яким повністю управляє користувач, надавачі послуг щодо віддаленого електронного підпису повинні застосовувати конкретні управлінські й адміністративні процедури безпеки та використовувати надійні системи і продукти, в тому числі безпечні канали електронного зв’язку, щоб гарантувати надійність середовища створення електронних підписів та використання його під одноосібним контролем підписувача. Якщо кваліфікований електронний підпис створено за допомогою засобу для створення віддаленого електронного підпису, то необхідно застосовувати вимоги до кваліфікованих надавачів довірчих послуг, установлені в цьому Регламенті.

(53) Призупинення чинності кваліфікованих сертифікатів є усталеною діючою практикою надавачів довірчих послуг у низці держав-членів, яка відрізняється від скасування і призводить до тимчасової втрати чинності сертифіката. Правова визначеність вимагає, щоб статус призупинення чинності сертифіката було завжди чітко зазначено. З такою метою на надавачів довірчих послуг необхідно покласти обов’язок чітко зазначати статус сертифіката

та, якщо чинність останнього призупинено, вказувати точний період, протягом якого чинність сертифіката буде призупинено. Цей Регламент не повинен покладати на надавачів довірчих послуг або держав-членів обов'язок застосовувати призупинення чинності, але повинен передбачати правила щодо прозорості у разі наявності такої практики.

(54) Транскордонна інтероперабельність і визнання кваліфікованих сертифікатів є передумовою для транскордонного визнання кваліфікованих електронних підписів. Тому кваліфіковані сертифікати не повинні підпадати під жодні обов'язкові вимоги, що перевищують вимоги, встановлені в цьому Регламенті. Проте на національному рівні необхідно дозволити включення до кваліфікованих сертифікатів конкретних характерних ознак, таких як унікальні ідентифікатори, за умови, що такі конкретні характерні ознаки не перешкоджають транскордонній інтероперабельності та визнанню кваліфікованих сертифікатів та електронних підписів.

(55) Сертифікація інформаційної безпеки на основі міжнародних стандартів, таких як ISO 15408, пов'язаних методів оцінювання та домовленостей щодо взаємного визнання є важливим інструментом для перевірки безпеки засобів для створення кваліфікованого електронного підпису, та необхідно сприяти її здійсненню. Проте такі інноваційні рішення і послуги, як підписання в мобільних пристроях та підписання в хмарі, залежать від технічних та організаційних рішень для тих засобів для створення кваліфікованого електронного підпису, для яких поки немає стандартів безпеки або для яких на разі проводять першу сертифікацію інформаційної безпеки. Рівень безпеки таких засобів для створення кваліфікованого електронного підпису може бути оцінено шляхом використання альтернативних процесів, лише якщо немає зазначених стандартів безпеки або на разі проводять першу сертифікацію інформаційної безпеки. Такі процеси повинні бути зіставними зі стандартами сертифікації інформаційної безпеки такою мірою, якою їхні рівні безпеки рівнозначні. Експертна оцінка може полегшити такі процеси.

(56) У цьому Регламенті необхідно встановити вимоги до засобів для створення кваліфікованого електронного підпису з метою забезпечення функціональності вдосконалених електронних підписів. Цей Регламент не повинен охоплювати все системне середовище, в якому функціонують такі пристрої. Тому сферу сертифікації засобів для створення кваліфікованого електронного підпису необхідно обмежити апаратним та програмним забезпеченням, використовуваним для управління даними для створення підписів, які створюють, зберігають або опрацьовують за допомогою засобу для створення підпису, та їх захисту. Як докладно зазначено у відповідних стандартах, сфера сертифікації не повинна поширюватися на застосунки для створення підписів.

(57) Для того, щоб забезпечити правову визначеність щодо чинності підпису, суттєвими є компоненти кваліфікованого електронного підпису, які повинна оцінити сторона-користувач, що здійснює валідацію. Крім того, визначення вимог до надавачів кваліфікованих довірчих послуг, які можуть надавати кваліфіковану послугу валідації сторонам-користувачам, які не бажають або не можуть самостійно здійснювати валідацію кваліфікованого електронного підпису, повинно стимулювати приватний та публічний сектор до інвестування в такі послуги. Обидві складові повинні полегшити та зробити зручнішою валідацію кваліфікованого електронного підпису для всіх осіб на рівні Союзу.

(58) Якщо транзакція передбачає використання юридичною особою кваліфікованої електронної печатки, кваліфікований електронний підпис уповноваженого представника юридичної особи необхідно прийняти рівнозначно.

(59) Електронні печатки повинні слугувати доказом того, що юридична особа видала електронний документ, забезпечуючи певність у походженні документа та цілісності.

(60) Надавачі довірчих послуг, які видають кваліфіковані сертифікати електронних печаток, повинні вжити необхідних заходів для того, щоб мати можливість встановити тотожність фізичної особи, яка представляє юридичну особу, якій надають кваліфікований сертифікат електронної печатки, якщо таке встановлення необхідне на національному рівні у контексті судових чи адміністративних проваджень.

(61) Цей Регламент повинен забезпечити довгострокове збереження інформації для забезпечення юридичної сили електронних підписів та електронних печаток протягом

тривалого часу та гарантування можливості їх валідації незалежно від технологічних змін в майбутньому.

(62) Для того, щоб забезпечити безпеку кваліфікованих позначок часу, цей Регламент повинен вимагати використання вдосконаленої електронної печатки, удосконаленого електронного підпису або інших рівнозначних методів. Можна передбачати, що інновації зможуть привести до появи нових технологій, які можуть забезпечити рівнозначний рівень безпеки для позначок часу. У разі використання методу, відмінного від удосконаленої електронної печатки або удосконаленого електронного підпису, надавачу кваліфікованих довірчих послуг необхідно довести у звіті про оцінювання відповідності, що такий метод забезпечує рівнозначний рівень безпеки та відповідає всім обов'язкам, установленим у цьому Регламенті.

(63) Електронні документи мають важливе значення для подальшого розвитку транскордонних електронних транзакцій на внутрішньому ринку. У цьому Регламенті необхідно встановити принцип, згідно з яким електронний документ не можна позбавити юридичної сили на підставі його електронної форми, щоб забезпечити неможливість відхилення електронної транзакції лише на підставі надання документа в електронній формі.

(64) Під час розгляду питання щодо форматів удосконалених електронних підписів і печаток Комісія повинна опиратися на чинні практики, стандарти та законодавство, зокрема на Рішення Комісії 2011/130/ЄС [(11)].

(65) Окрім автентифікації документа, що його видала юридична особа, електронні печатки можуть використовувати для автентифікації будь-яких цифрових активів юридичної особи, таких як код програмного забезпечення або сервери.

(66) Суттєвим є передбачення правових рамок для полегшення транскордонного визнання між наявними національними правовими системами, пов'язаними з послугами реєстрованої електронної доставки. Такі рамки могли б відкрити також нові ринкові можливості для надавачів довірчих послуг ЄС пропонувати нові пан'європейські послуги реєстрованої електронної доставки.

(67) Послуги автентифікації веб-сайту надають засоби, за допомогою яких відвідувач веб-сайту може переконатися, що за веб-сайтом стоїть реальний і легітимний суб'єкт. Такі послуги сприяють побудові довіри і впевненості у межах провадження підприємницької діяльності онлайн, оскільки користувачі матимуть упевненість у справжності автентифікованого веб-сайту. Надання і використання послуг автентифікації веб-сайту є повністю добровільними. Проте для того, щоб автентифікація веб-сайту стала засобом підвищення довіри, давала користувачеві найкращий досвід та сприяла росту внутрішнього ринку, у цьому Регламенті необхідно встановити для надавачів та їхніх послуг мінімальні обов'язки щодо безпеки та відповідальності. Для такого було враховано результати наявних галузевих ініціатив (наприклад, Certification Authorities/Browsers Forum (CA/B Forum) (Форум органів сертифікації/розробників браузерів)). Крім того, цей Регламент не повинен заважати використанню інших засобів або методів для автентифікації веб-сайту, на які не розповсюджується дія цього Регламенту, та не повинен перешкоджати надавачам послуг автентифікації веб-сайту з третіх країн надавати свої послуги клієнтам у Союзі. Проте послуги автентифікації веб-сайту, що їх надає надавач з третьої країни, необхідно визнати кваліфікованими відповідно до цього Регламенту, лише якщо між Європейським Союзом та країною заснування надавача укладено міжнародну угоду.

(68) Поняття «юридична особа», відповідно до положень Договору про функціонування Європейського Союзу щодо заснування, надає учасникам ринку можливість вільно вибрати організаційно-правову форму, яку вони вважають доцільною для провадження своєї діяльності. Відповідно, у розумінні Договору про функціонування ЄС «юридична особа» означає будь-який суб'єкт, що його створено згідно з правом держави-члена або діяльність якого регулює право держави-члена, незалежно від його організаційно-правової форми.

(69) Установи, органи, офіси та агентства Європейського Союзу заохочують визнавати електронну ідентифікацію та довірчі послуги, охоплені цим Регламентом, для цілей адміністративної співпраці, користуючись, зокрема, вигодами наявних належних практик та результатів поточних проектів у сферах, охоплених цим Регламентом.

(70)Для того, щоб доповнити певні детальні технічні аспекти цього Регламенту у гнучкий та швидкий спосіб, Комісію необхідно наділити повноваженням ухвалювати акти відповідно до статті 290 Договору про функціонування ЄС щодо критеріїв, яким повинні відповідати органи, відповідальні за сертифікацію засобів для створення кваліфікованого електронного підпису. Особливо важливим є проведення Комісією належних консультацій під час підготовчої роботи, у тому числі на рівні експертів. Під час підготування та розроблення проектів делегованих актів, Комісія повинна забезпечити одночасне, своєчасне та належне передання відповідних документів до Європейського Парламенту і Ради.

(71)Для того, щоб забезпечити уніфіковані умови для імплементації цього Регламенту, Комісію необхідно наділити виконавчими повноваженнями, зокрема для визначення вихідних номерів стандартів, використання яких створить презумпцію відповідності певним вимогам, установленим у цьому Регламенті. Такі повноваження необхідно здійснювати згідно з Регламентом Європейського Парламенту і Ради (ЄС) № 182/2011 [(12)].

(72)Під час ухвалення делегованих або імплементаційних актів, Комісії необхідно належним чином враховувати стандарти та технічні специфікації, що їх розробили європейські та міжнародні організації та органи стандартизації, зокрема Європейський комітет зі стандартизації, Європейський інститут телекомунікаційних стандартів, Міжнародна організація зі стандартизації та Міжнародний союз електрозв'язку з метою забезпечення високого рівня безпеки та інтероперабельності електронної ідентифікації та довірчих послуг.

(73)З міркувань правової визначеності та чіткості Директиву 1999/93/ЄС необхідно скасувати.

(74)Для того, щоб забезпечити правову визначеність для учасників ринку, які вже використовують кваліфіковані сертифікати, видані фізичним особам відповідно до Директиви 1999/93/ЄС, необхідно передбачити достатній строк для перехідних цілей. У схожий спосіб необхідно встановити заходи перехідного характеру для безпечних засобів для створення підписів, відповідність яких визначено відповідно до Директиви 1999/93/ЄС, а також для надавачів послуг сертифікації, що видадуть кваліфіковані сертифікати, до 1 липня 2016 року. Нарешті, також необхідно забезпечити Комісію засобами для ухвалення імплементаційних та делегованих актів до зазначеної дати.

(75)Дати застосування, викладені в цьому Регламенті, не впливають на наявні обов'язки, покладені на держави-члени за правом Союзу, зокрема за Директивою 2006/123/ЄС.

(76)Оскільки цілі цього Регламенту не може бути достатньою мірою досягнуто державами-членами, але може бути, з огляду на масштаб діяльності, краще досягнуто на рівні Союзу, Союз може ухвалювати інструменти згідно з принципом субсидіарності, як зазначено у статті 5 Договору про Європейський Союз. Відповідно до принципу пропорційності, визначеного у згаданій статті, цей Регламент не виходить за межі того, що необхідно для досягнення таких цілей.

(77)Згідно зі статтею 28(2) Регламенту Європейського Парламенту і Ради (ЄС) № 45/2001 [(13)] проведено консультації з Уповноваженим Європейської Комісії із захисту даних, який надав висновок 27 вересня 2012 року [(14)],

УХВАЛИЛИ ЦЕЙ РЕГЛАМЕНТ:

## ГЛАВА I
## ЗАГАЛЬНІ ПОЛОЖЕННЯ

*Стаття 1*

**Предмет**

Для цілей забезпечення належного функціонування внутрішнього ринку, маючи разом з цим на меті досягнення належного рівня безпеки засобів електронної ідентифікації та довірчих послуг, у цьому Регламенті:

(a) встановлено умови, на яких держави-члени визнають засоби електронної ідентифікації фізичних та юридичних осіб, що їх охоплює нотифікована схема електронної ідентифікації

іншої держави-члена;

(b) встановлено правила щодо довірчих послуг, зокрема щодо електронних транзакцій; та

(c) встановлено правові рамки для електронних підписів, електронних печаток, електронних позначок часу, електронних документів, послуг реєстрованої електронної доставки та послуг з надання сертифікатів для автентифікації веб-сайтів.

*Стаття 2*

**Сфера застосування**

1. Цей Регламент застосовують до схем електронної ідентифікації, що їх нотифікувала держава-член, та до надавачів довірчих послуг, заснованих у Союзі.

2. Цей Регламент не застосовують до надання довірчих послуг, що їх використовують винятково в закритих системах, що з'являються на підставі національного права або угод між визначеною групою учасників.

3. Цей Регламент не впливає на національне право або право Союзу, пов'язане з укладанням та чинністю договорів або інших юридичних чи процесуальних обов'язків, пов'язаних із формою.

*Стаття 3*

**Терміни та означення**

Для цілей цього Регламенту застосовують такі терміни та означення:

(1) «електронна ідентифікація» означає процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну особу, або юридичну особу, або фізичну особу, що представляє юридичну особу;

(2) «засіб електронної ідентифікації» означає матеріальну та/або нематеріальну одиницю, яка містить ідентифікаційні дані особи і яку використовують для автентифікації в онлайн-послугах;

(3) «ідентифікаційні дані особи» означають сукупність даних, що дає змогу встановити тотожність фізичної особи, або юридичної особи, або фізичної особи, що представляє юридичну особу;

(4) «схема електронної ідентифікації» означає систему електронної ідентифікації, у межах якої засоби електронної ідентифікації випускають для фізичних осіб, або юридичних осіб, або фізичних осіб, що представляють юридичних осіб;

(5) «автентифікація» означає електронний процес, що дає змогу підтвердити електронну ідентифікацію фізичної або юридичної особи або походження та цілісність даних в електронній формі;

(6) «сторона-користувач» означає фізичну або юридичну особу, яка покладається на електронну ідентифікацію або довірчу послугу;

(7) «орган публічного сектора» означає державний, регіональний або місцевий орган влади, орган публічного права або асоціацію, утворену одним або декількома органами влади, одним або декількома органами публічного права, або приватну особу, уповноважену принаймні одним з таких органів влади, органів або асоціацій надавати публічні послуги, якщо останні діють у межах такого повноваження;

(8) «орган публічного права» означає орган, визначений у пункті 4 статті 2(1) Директиви Європейського Парламенту і Ради 2014/24/ЄС [(15)];

(9) «підписувач» означає фізичну особу, яка створює електронний підпис;

(10) «електронний підпис» означає дані в електронній формі, які додають до інших даних в електронній формі або логічно пов'язують з ними і які використовує підписувач для підписання;

(11) «удосконалений електронний підпис» означає електронний підпис, який відповідає вимогам,

викладеним у статті 26;

(12)«кваліфікований електронний підпис» означає удосконалений електронний підпис, який створюють за допомогою засобу для створення кваліфікованого електронного підпису і який ґрунтується на кваліфікованому сертифікаті електронних підписів;

(13)«дані для створення електронного підпису» означають унікальні дані, які використовує підписувач для створення електронного підпису;

(14)«сертифікат електронного підпису» означає електронне свідоцтво, що зв'язує дані для валідації електронного підпису з фізичною особою та підтверджує щонайменше прізвище й ім'я або псевдонім такої особи;

(15)«кваліфікований сертифікат електронного підпису» означає сертифікат електронного підпису, що його видає кваліфікований надавач довірчих послуг і який відповідає вимогам, установленим у додатку I;

(16)«довірча послуга» означає електронну послугу, яку зазвичай надають за винагороду і яка охоплює:

(a) створення, верифікацію та валідацію електронних підписів, електронних печаток або електронних позначок часу, послуг реєстрованої електронної доставки та сертифікатів, пов'язаних з такими послугами; або

(b) створення, верифікацію та валідацію сертифікатів автентифікації веб-сайту; або

(c) зберігання електронних підписів, електронних печаток або сертифікатів, пов'язаних з такими послугами;

(17)«кваліфікована довірча послуга» означає довірчу послугу, яка відповідає застосовним вимогам, установленим у цьому Регламенті;

(18)«орган з оцінювання відповідності» означає орган, визначений у пункті 13 статті 2 Регламенту (ЄС) № 765/2008 та акредитований відповідно до зазначеного Регламенту як орган, компетентний в оцінюванні відповідності кваліфікованого надавача довірчих послуг та надаваних ним кваліфікованих довірчих послуг;

(19)«надавач довірчих послуг» означає фізичну або юридичну особу, яка надає одну або декілька довірчих послуг як кваліфікований або некваліфікований надавач довірчих послуг;

(20)«кваліфікований надавач довірчих послуг» означає надавача довірчих послуг, який надає одну або декілька кваліфікованих довірчих послуг та має статус кваліфікованого, що його надав наглядовий орган;

(21)«продукт» означає апаратне або програмне забезпечення чи його відповідні компоненти, призначені для використання у межах надання довірчих послуг;

(22)«засіб для створення електронного підпису» означає налаштоване програмне або апаратне забезпечення, яке використовують для створення електронного підпису;

(23)«засіб для створення кваліфікованого електронного підпису» означає засіб для створення електронного підпису, що відповідає вимогам, установленим у додатку II;

(24)«створювач печатки» означає юридичну особу, яка створює електронну печатку;

(25)«електронна печатка» означає дані в електронній формі, які додаються до інших даних в електронній формі або логічно пов'язують з ними для забезпечення походження та цілісності останніх;

(26)«удосконалена електронна печатка» означає електронну печатку, яка відповідає вимогам, викладеним у статті 36;

(27)«кваліфікована електронна печатка» означає удосконалену електронну печатку, яку створюють за допомогою засобу для створення кваліфікованої електронної печатки і яка ґрунтується на кваліфікованому сертифікаті електронної печатки;

(28)«дані для створення електронної печатки» означають унікальні дані, які використовує створювач електронної печатки для створення електронної печатки;

(29)«сертифікат електронної печатки» означає електронне свідоцтво, що пов’язує дані для валідації електронної печатки з юридичною особою та підтверджує найменування цієї особи;

(30)«кваліфікований сертифікат електронної печатки» означає сертифікат електронної печатки, що його видає кваліфікований надавач довірчих послуг і який відповідає вимогам, установленим у додатку III;

(31)«засіб для створення електронної печатки» означає налаштоване програмне або апаратне забезпечення, яке використовують для створення електронних печаток;

(32)«засіб для створення кваліфікованої електронної печатки» означає засіб для створення електронної печатки, який відповідає mutatis mutandis вимогам, установленим у додатку II;

(33)«електронна позначка часу» означає дані в електронній формі, які пов’язують інші електронні дані з певним моментом часу, надаючи доказ того, що останні існували в той час;

(34)«кваліфікована електронна позначка часу» означає електронну позначку часу, яка відповідає вимогам, установленим у статті 42;

(35)«електронний документ» означає будь-який контент, який зберігають в електронній формі, зокрема текст або звук, візуальний або аудіовізуальний запис;

(36)«послуга реєстрованої електронної доставки» означає послугу, яка дає змогу передавати дані між третіми особами за допомогою електронних засобів, надає докази, пов’язані з опрацюванням переданих даних, у тому числі підтвердження відправлення та отримання даних, і захищає передані дані від ризику втрати, викрадення, пошкодження або несанкціонованих змін;

(37)«кваліфікована послуга реєстрованої електронної доставки» означає послугу реєстрованої електронної доставки, яка відповідає вимогам, установленим у статті 44;

(38)«сертифікат автентифікації веб-сайту» означає свідоцтво, яке дає змогу автентифікувати веб-сайт та пов’язує веб-сайт з фізичною або юридичною особою, якій видали сертифікат;

(39)«кваліфікований сертифікат автентифікації веб-сайту» означає сертифікат автентифікації веб-сайту, що його видає кваліфікований надавач довірчих послуг і який відповідає вимогам, установленим у додатку IV;

(40)«дані для валідації» означають дані, які використовують для валідації електронного підпису або електронної печатки;

(41)«валідація» означає процес верифікації та підтвердження дійсності електронного підпису або електронної печатки.

*Стаття 4*

**Принцип внутрішнього ринку**

1. Не повинно існувати жодних обмежень для надання довірчих послуг на території однієї держави-члена надавачем довірчих послуг, заснованим у іншій державі-члені, з причин, що належать до сфер, на які розповсюджується дія цього Регламенту.

2. Продукти та довірчі послуги, що відповідають вимогам цього Регламенту, допускають до вільного обігу на внутрішньому ринку.

*Стаття 5*

**Опрацювання та захист даних**

1. Опрацювання персональних даних здійснюють відповідно до Директиви 95/46/ЄС.

2. Без обмеження юридичної сили, надаваної псевдонімам за національним правом, використання псевдонімів в електронних транзакціях не забороняють.

## ГЛАВА II

## ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ

*Стаття 6*

**Взаємне визнання**

1. Якщо для доступу до онлайн-послуги, яку надає орган публічного сектора онлайн у будь-якій державі-члені, національне право або адміністративна практика вимагають електронної ідентифікації за допомогою засобів електронної ідентифікації та автентифікації, засоби електронної ідентифікації, випущені в іншій державі-члені, визнає перша держава-член для цілей транскордонної автентифікації тієї онлайн послуги за умови дотримання таких умов:

(a) засоби електронної ідентифікації випускають за схемою електронної ідентифікації, внесеною у список, що його опублікувала Комісія відповідно до статті 9;

(b) рівень надійності засобів електронної ідентифікації відповідає рівню надійності, який вимагає відповідний орган публічного сектора для доступу до такої послуги онлайн в першій державі-члені, або вищий, ніж такий рівень, за умови відповідності рівня надійності засобів електронної ідентифікації рівню надійності «істотний» або «високий»;

(c) відповідний орган публічного сектора використовує рівень надійності «істотний» або «високий» для доступу до такої послуги онлайн.

Таке визнання здійснюють не пізніше ніж через 12 місяців після опублікування Комісією списку, зазначеного в пункті (a) першого підпараграфа.

2. Засіб електронної ідентифікації, який випускають за схемою електронної ідентифікації, внесеною у список, що його опублікувала Комісія відповідно до статті 9, і який відповідає рівню надійності «низький», можуть визнати органи публічного сектора для цілей транскордонної автентифікації послуг, які надають такі органи онлайн.

*Стаття 7*

**Прийнятність схем електронної ідентифікації для нотифікації**

Схему електронної ідентифікації може бути нотифіковано відповідно до статті 9(1), якщо виконано такі умови:

(a) засоби електронної ідентифікації за схемою електронної ідентифікації випускають:

  (i) державою-членом, що здійснює нотифікацію;

  (ii) за дорученням держави-члена, що здійснює нотифікацію, або

  (iii) незалежно від держави-члена, що здійснює нотифікацію, але така держава-член визнає їх;

(b) засоби електронної ідентифікації, які випускають за схемою електронної ідентифікації, можуть використовуватися для доступу щонайменше до однієї послуги, яку надає орган публічного сектора і яка вимагає електронної ідентифікації на території держави-члена, що здійснює нотифікацію;

(c) схема електронної ідентифікації та засоби електронної ідентифікації, які випускають за нею, відповідають вимогам щонайменше одного з рівнів надійності, які встановлено в імплементаційному акті, зазначеному в статті 8(3);

(d) держава-член, що здійснює нотифікацію, забезпечує присвоєння ідентифікаційних даних особи, які однозначно представляють відповідну особу, зазначеній у пункті 1 статті 3 фізичній або юридичній особі в момент випуску за такою схемою засобу електронної ідентифікації відповідно до технічних вимог, стандартів та процедур щодо відповідного рівня надійності, передбачених в імплементаційному акті, зазначеному у статті 8(3);

(e) особа, яка випускає засоби електронної ідентифікації за такою схемою, забезпечує присвоєння засобів електронної ідентифікації зазначеній у пункті (d) цієї статті особі відповідно до технічних вимог, стандартів та процедур щодо відповідного рівня надійності, передбачених в імплементаційному акті, зазначеному у статті 8(3);

(f) держава-член, що здійснює нотифікацію, забезпечує наявність автентифікації онлайн у такий спосіб, щоб будь-яка сторона-користувач, заснована в іншій державі-члені, мала можливість підтвердити ідентифікаційні дані особи в електронній формі.

Для сторін-користувачів, відмінних від органів публічного сектора, держава-член, що здійснює нотифікацію, може визначати умови доступу до такої автентифікації. Транскордонну автентифікацію здійснюють безкоштовно, якщо її проводять у зв'язку з онлайн-послугою, що її надає орган публічного сектора.

Держави-члени не повинні висувати жодних конкретних непропорційних технічних вимог до сторін-користувачів, які мають намір провести таку автентифікацію, якщо такі вимоги запобігають або значною мірою перешкоджають інтероперабельності нотифікованих схем електронної ідентифікації;

(g) щонайменше за шість місяців до нотифікації відповідно до статті 9(1) держава-член, що здійснює нотифікацію, надає іншим державам-членам для цілей обов'язку, визначеного у статті 12(5), опис схеми відповідно до процедурного порядку, встановленого в імплементаційних актах, зазначених у статті 12(7);

(h) схема електронної ідентифікації відповідає вимогам імплементаційного акту, зазначеного в статті 12(8).

*Стаття 8*

**Рівні надійності схем електронної ідентифікації**

1. У схемі електронної ідентифікації, нотифікованій відповідно до статті 9(1), визначають низький, істотний та/або високий рівні надійності для засобів електронної ідентифікації, що їх випускають за такою схемою.

2. Низький, істотний та високий рівні надійності повинні відповідати таким критеріям:

(a) низький рівень надійності стосується засобу електронної ідентифікації в контексті схеми електронної ідентифікації, який забезпечує обмежений ступінь довіри до заявленої або стверджуваної тотожності особи, та охарактеризований на основі технічних специфікацій, пов'язаних із ними стандартів та процедур, у тому числі технічні засоби контролю, ціль яких полягає в зниженні ризику неправильного використання або зміни тотожності особи;

(b) істотний рівень надійності стосується засобу електронної ідентифікації в контексті схеми електронної ідентифікації, який забезпечує істотний ступінь довіри до заявленої або стверджуваної тотожності особи, та охарактеризований на основі технічних специфікацій, пов'язаних з ними стандартів та процедур, у тому числі технічні засоби контролю, ціль яких полягає в істотному зниженні ризику неправильного використання або зміни тотожності особи;

(c) високий рівень надійності стосується засобу електронної ідентифікації в контексті схеми електронної ідентифікації, який забезпечує вищий ступінь довіри до заявленої або стверджуваної тотожності особи, порівняно із засобом електронної ідентифікації, що має істотний рівень довіри, та охарактеризований на основі технічних специфікацій, пов'язаних з ними стандартів та процедур, у тому числі технічні засоби контролю, ціль яких полягає у запобіганні неправильному використанню або зміні тотожності особи.

3. До 18 вересня 2015 року, беручи до уваги відповідні міжнародні стандарти та відповідно до параграфа 2, Комісія шляхом ухвалення імплементаційних актів установлює мінімальні технічні специфікації, стандарти та процедури, на основі яких визначають низький, істотний та високий рівні надійності для засобів електронної ідентифікації для цілей параграфа 1.

Такі мінімальні технічні специфікації, стандарти та процедури повинні бути встановлені на основі надійності та якості таких складових:

(a) процедури доведення та верифікації тотожності фізичних або юридичних осіб, які подали заявку на випуск для них засобів електронної ідентифікації;

(b) процедури випуску засобів електронної ідентифікації, на які подавали заявку;

(c) механізму автентифікації, за допомогою якого фізична або юридична особа використовує

засіб електронної ідентифікації для підтвердження стороні-користувачу своєї тотожності;

(d) суб'єкта, який випускає засоби електронної ідентифікації

(e) будь-якого іншого суб'єкта, який бере участь в опрацюванні заявки на випуск засобів електронної ідентифікації, та

(f) технічних специфікацій і специфікацій щодо безпеки випущених засобів електронної ідентифікації.

Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 9*

**Нотифікація**

1. Держава-член, що здійснює нотифікацію, нотифікує без зайвих зволікань Комісії таку інформацію та подальші зміни до неї:

(a) опис схеми електронної ідентифікації, у тому числі її рівні надійності та орган, що випускає засоби електронної ідентифікації за такою схемою;

(b) застосовний режим нагляду та інформацію про режим відповідальності щодо:

(i) сторони, яка випускає засоби електронної ідентифікації, та

(ii) сторони, яка проводить процедуру автентифікації;

(c) орган або органи, відповідальні за схему електронної ідентифікації;

(d) інформацію про суб'єкта або суб'єктів, які управляють реєстрацією унікальних ідентифікаційних даних особи;

(e) опис дотримання вимог імплементаційних актів, зазначених у статті 12(8);

(f) опис автентифікації, зазначеної в пункті (f) статті 7;

(g) порядок призупинення чинності або скасування нотифікованої схеми ідентифікації, автентифікації або їхніх відповідних сумнівних частин.

2. Через один рік з дати застосування імплементаційних актів, зазначених у статтях 8(3) та 12(8), Комісія повинна опубліковувати в *Офіційному віснику Європейського Союзу* список схем електронної ідентифікації, які нотифіковано на підставі параграфа 1 цієї статті, та основну пов'язану з ними інформацію.

3. Якщо Комісія отримає нотифікацію після закінчення строку, зазначеного в параграфі 2, вона повинна опубліковувати в *Офіційному віснику Європейського Союзу* зміни до списку, зазначеного в параграфі 2, протягом двох місяців з моменту отримання нотифікації.

4. Держава-член може подати до Комісії прохання на видалення власної схеми ідентифікації зі списку, зазначеного в параграфі 2. Комісія повинна опубліковувати в *Офіційному віснику Європейського Союзу* відповідні зміни у списку протягом одного місяця з дня отримання прохання від держави-члена.

5. Комісія може шляхом ухвалення імплементаційних актів визначити обставини, формати і процедури нотифікацій за параграфом 1. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 10*

**Порушення безпеки**

1. Якщо схему електронної ідентифікації, нотифіковану відповідно до статті 9(1), або автентифікацію, зазначену в пункті (f) статті 7, порушують або частково компрометують у такий спосіб, що це впливає на надійність транскордонної автентифікації такої схеми, держава-член, що здійснює нотифікацію, невідкладно призупиняє чинність транскордонної автентифікації або її скомпрометованих частини чи скасовує їх та інформує про це інші держави-члени і Комісію.

2. Якщо порушення або компрометацію, зазначені в параграфі 1, усунуто, держава-член, що здійснює нотифікацію, поновлює транскордонну автентифікацію та інформує про це інші держави-члени і Комісію без зайвих зволікань.

3. Якщо порушення або компрометацію, зазначені в параграфі 1, не усунуто протягом 3 місяців після призупинення чинності або скасування схеми, держава-член, що здійснює нотифікацію, інформує інші держави-члени і Комісію про скасування схеми електронної ідентифікації.

Комісія публікує в *Офіційному віснику Європейського Союзу* відповідні зміни до списку, зазначеного в статті 9(2), без зайвих зволікань.

*Стаття 11*

**Відповідальність**

1. Держава-член, яка здійснює нотифікацію, несе відповідальність за шкоду, спричинену будь-якій фізичній або юридичній особі навмисно чи з необережності через невиконання своїх обов'язків, зазначених у пунктах (d) і (f) статті 7, у межах транскордонної транзакції.

2. Сторона, яка випускає засоби електронної ідентифікації, несе відповідальність за шкоду, спричинену будь-якій фізичній чи юридичній особі навмисно чи з необережності через невиконання свого обов'язку, зазначеного у пункті (e) статті 7, у межах транскордонної транзакції.

3. Сторона, яка проводить процедуру автентифікації, несе відповідальність за шкоду, спричинену будь-якій фізичній чи юридичній особі навмисно чи з необережності через незабезпечення правильного проведення автентифікації, зазначеної в пункті (f) статті 7, у межах транскордонної транзакції.

4. Параграфи 1, 2 і 3 застосовують відповідно до національних правил щодо відповідальності.

5. Параграфи 1, 2 і 3 не обмежують відповідальність за національним правом сторін транзакції, у межах якої використовують засоби електронної ідентифікації, що належать до схеми електронної ідентифікації, нотифікованої відповідно до статті 9(1).

*Стаття 12*

**Співпраця та інтероперабельність**

1. Національні схеми електронної ідентифікації, нотифіковані відповідно до статті 9(1), повинні бути інтероперабельними.

2. Для цілей параграфа 1 необхідно встановити рамки інтероперабельності.

3. Рамки інтероперабельності повинні відповідати таким критеріям:

(a) мати на меті збереження технологічного нейтралітету і не виділяти будь-які національні технічні рішення щодо електронної ідентифікації в межах держави-члена;

(b) відповідати європейським та міжнародним стандартам, за можливості;

(c) полегшувати впровадження принципу приватності за призначенням;

(d) забезпечувати опрацювання персональних даних відповідно до Директиви 95/46/ЄС.

4. Рамки інтероперабельності повинні містити:

(a) покликання на мінімальні технічні вимоги, пов'язані з рівнями надійності відповідно до статті 8;

(b) опис відповідності національних рівнів надійності нотифікованих схем електронної ідентифікації рівням надійності, зазначеним у статті 8;

(c) покликання на мінімальні технічні вимоги до інтероперабельності;

(d) покликань на мінімальні набори ідентифікаційних даних особи, які однозначно визначають фізичну або юридичну особу та які доступі в схемах електронної ідентифікації;

(e) процедурні правила;

(f) механізми врегулювання спорів та

(g) спільні експлуатаційні стандарти безпеки.

5. Держави-члени співпрацюють із таких питань:

(a) інтероперабельність схем електронної ідентифікації, нотифікованих відповідно до статті 9(1), та схем електронної ідентифікації, які держави-члени мають намір нотифікувати, та

(b) безпеки схем електронної ідентифікації.

6. Співпраця між державами-членами охоплює:

(a) обмін інформацією, досвідом і належною практикою щодо схем електронної ідентифікації, зокрема щодо технічних вимог, пов'язаних з інтероперабельністю та рівнями надійності;

(b) обмін інформацією, досвідом і належною практикою щодо роботи з рівнями надійності схем електронної ідентифікації відповідно до статті 8;

(c) експертної оцінки схем електронної ідентифікації, на які розповсюджується дія цього Регламенту, та

(d) дослідження відповідних змін у секторі електронної ідентифікації.

7. До 18 березня 2015 року Комісія шляхом ухвалення імплементаційних актів установлює процедурні механізми сприяння співпраці між державами-членами, про яку йдеться в параграфах 5 і 6, з метою досягнення високого рівня довіри і безпеки, що доцільний для ступеня ризику.

8. До 18 вересня 2015 року, з метою встановлення уніфікованих умов для впровадження вимоги за параграфом 1, Комісія ухвалює імплементаційні акти щодо рамок інтероперабельності, як це викладено в параграфі 4, відповідно до викладених у параграфі 3 критеріїв та беручи до уваги результати співпраці між державами-членами.

9. Імплементаційні акти, зазначені в параграфах 7 і 8 цієї статті, ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

## ГЛАВА III
## ДОВІРЧІ ПОСЛУГИ

### *СЕКЦІЯ 1*
### *Загальні положення*

*Стаття 13*

**Відповідальність і тягар доказування**

1. Без обмеження параграфа 2, надавачі довірчих послуг несуть відповідальність за шкоду, спричинену навмисно або з необережності будь-якій фізичній чи юридичній особі через невиконання обов'язків, передбачених у цьому Регламенті.

Тягар доказування умислу або необережності некваліфікованого надавача довірчих послуг покладають на фізичну або юридичну особу, яка заявляє про шкоду, зазначену в першому підпараграфі.

Припускають наявність умислу або необережності кваліфікованого надавача довірчих послуг, якщо кваліфікований надавач довірчих послуг не доведе, що шкоди, зазначена в першому підпараграфі, завдано не через умисел або необережність такого кваліфікованого надавача довірчих послуг.

2. Якщо надавачі довірчих послуг у належний спосіб та заздалегідь поінформують своїх користувачів про обмеження у використанні надаваних ними послуг і якщо треті особи можуть визнати такі обмеження, надавачі довірчих послуг не несуть відповідальності за шкоду, що виникла внаслідок використання послуг з перевищенням зазначених обмежень.

3. Параграфи 1 і 2 застосовують відповідно до національних правил щодо відповідальності.

*Стаття 14*

**Міжнародні аспекти**

1. Довірчі послуги, що їх надають надавачі довірчих послуг, засновані в третій країні, визнають юридично рівнозначними довірчим послугам, які надають кваліфіковані надавачі довірчих послуг, засновані у Союзі, якщо довірчі послуги, які походять із третьої країни, визнано за угодою, укладеною між Союзом та такою третьою країною або міжнародною організацією відповідно до статті 218 Договору про функціонування Європейського Союзу.

2. Зазначені в параграфі 1 угоди забезпечують, зокрема:

(a) відповідність вимогам, застосовним до кваліфікованих надавачів довірчих послуг, заснованих у Союзі, та до кваліфікованих довірчих послуг, які вони надають, надавачів довірчих послуг у третій країні або міжнародних організацій, з якими укладено угоди, та довірчих послуг, які вони надають;

(b) кваліфіковані довірчі послуги, які надають кваліфіковані надавачі довірчих послуг, засновані у Союзі, визнано юридично рівнозначними довірчим послугам, які надають надавачі довірчих послуг у третій країні чи міжнародні організації, з якими укладено угоду.

*Стаття 15*

**Доступність для осіб з інвалідністю**

За можливості, довірчі послуги та продукти для кінцевих користувачів, використовувані під час надання таких послуг, повинні бути доступними для осіб з інвалідністю.

*Стаття 16*

**Санкції**

Держави-члени встановлюють правила застосування санкцій у разі порушень цього Регламенту. Передбачені санкції повинні бути ефективними, пропорційними та стримувальними.

***СЕКЦІЯ 2***

***Нагляд***

*Стаття 17*

**Наглядовий орган**

1. Держави-члени призначають наглядовий орган, заснований на їхній території, або за взаємною домовленістю з іншою державою-членом наглядовий орган, заснований у такій іншій державі-члені. Такий орган відповідальний за виконання завдань із нагляду в державі-члені, яка його призначила.

Наглядовим органам надають необхідні повноваження та належні ресурси для виконання їхніх завдань.

2. Держави-члени повідомляють Комісії назви та адреси своїх відповідних призначених наглядових органів.

3. Роль наглядового органу є такою:

(a) здійснення нагляду за кваліфікованими надавачами довірчих послуг, заснованих у державі-члені, що призначила наглядовий орган, у межах наглядової діяльності *ex ante* та *ex post* для того, щоб такі кваліфіковані надавачі довірчих послуг та надавані ними кваліфіковані довірчі послуги відповідали вимогам, установленим у цьому Регламенті;

(b) за необхідності, вжиття заходів до некваліфікованих надавачів довірчих послуг, заснованих у державі-члені, що призначила наглядовий орган, у межах наглядової діяльності *ex post* після

отримання інформації про те, що некваліфіковані надавачі довірчих послуг або надавані ними довірчі послуги нібито не відповідають вимогам, установленим у цьому Регламенті.

4. Для цілей параграфа 3 та з урахуванням передбачених у ньому обмежень, завдання наглядового органу охоплюють, зокрема:

(a) співпрацю з іншими наглядовими органами та надання допомоги їм відповідно до статті 18;

(b) аналізування звітів про оцінювання відповідності, зазначених у статтях 20(1) і 21(1);

(c) інформування інших наглядових органів та широкого загалу про порушення безпеки або втрату цілісності відповідно до статті 19(2);

(d) звітування перед Комісією про свою основну діяльність відповідно до параграфа 6 цієї статті;

(e) проведення аудитів або подання запиту до органу з оцінювання відповідності на проведення оцінювання відповідності кваліфікованого надавача довірчих послуг відповідно до статті 20(2);

(f) співпрацю з органами з питань захисту даних, зокрема, шляхом їх інформування без зайвих зволікань про результати аудитів кваліфікованих надавачів довірчих послуг, якщо виявлено, що правила захисту персональних даних порушено;

(g) надання надавачам довірчих послуг та надаваних ними послугам статусу кваліфікованих та відкликання цього статусу відповідно до статей 20 і 21;

(h) інформування органу, відповідального за національний довірчий список відповідно до статті 22(3), свої рішення про надання або відкликання статусу кваліфікованого, якщо цей орган не є наглядовим;

(i) перевірку наявності і правильного застосування положень щодо планів припинення діяльності у разі припинення кваліфікованими надавачами довірчих послуг своєї діяльності, у тому числі способи доступності до інформації, що зберігається, відповідно до пункту (h) статті 24(2);

(j) вимагання від надавачів довірчих послуг усунення будь-якого невиконання вимог, установлених у цьому Регламенті.

5. Держави-члени можуть вимагати від наглядового органу встановлення, підтримки та оновлення інфраструктури довіри відповідно до умов, установлених у національному праві.

6. До 31 березня кожного року кожний наглядовий орган надає Комісії звіт про основні напрямки своєї діяльності за попередній календарний рік разом зі стислим викладом отриманих від надавачів довірчих послуг повідомлень про порушення відповідно до статті 19(2).

7. Комісія надає річний звіт, зазначений у параграфі 6, усім державам-членам.

8. Комісія може шляхом ухвалення імплементаційних актів визначити формати і процедури для звіту, зазначеного в параграфі 6. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 18*

**Взаємна допомога**

1. Наглядові органи співпрацюють для обміну належною практикою.

Наглядовий орган, після отримання обґрунтованого запиту від іншого наглядового органу, надає такому органу допомогу у такий спосіб, щоб діяльність наглядових органів можна було здійснювати узгоджено. Взаємна допомога може охоплювати, зокрема, інформаційні запити і наглядові заходи, такі як запити на проведення інспекцій, пов’язаних зі звітами про оцінювання відповідності, зазначеними в статтях 20 і 21.

2. Наглядовий орган, якому направлено запит на надання допомоги, може відхилити цей запит за будь-якої з таких умов:

(a) наглядовий орган не має права надавати допомогу, на надання якої надійшов запит;

(b) допомога, на надання якої надійшов запит, не є пропорційною наглядовій діяльності наглядового органу, проваджуваній відповідно до статті 17;

(c) надання допомоги, на надання якої надійшов запит, буде несумісним з цим Регламентом.

3. За доцільності, держави-члени можуть уповноважити свої відповідні наглядові органи здійснювати спільні розслідування із залученням працівників наглядових органів інших держав-членів. Домовленості і процедури для таких спільних заходів узгоджують і встановлюють держави-члени відповідно до свого національного права.

*Стаття 19*

**Вимоги до безпеки, застосовні до надавачів довірчих послуг**

1. Кваліфіковані і некваліфіковані надавачі довірчих послуг вживають відповідних технічних та організаційних заходів для управління ризиками, яким піддається безпека надаваних ними довірчих послуг. Беручи до уваги останні технічні досягнення, такі заходи повинні забезпечити сумірність рівня безпеки ступеню ризику. Зокрема, необхідно вжити заходів для запобігання впливу інцидентів у сфері безпеки, їх мінімізації та інформування стейкхолдерів про негативні наслідки будь-яких таких інцидентів.

2. Кваліфіковані і некваліфіковані надавачі довірчих послуг повідомляють наглядовий орган та, за доцільності, інші відповідні органи, такі як компетентний національний орган із інформаційної безпеки або орган з питань захисту даних, про будь-які порушення безпеки або втрату цілісності, які мають істотний вплив на надавану довірчу послугу або на персональні дані, використовувані у її межах, без зайвих зволікань та в будь-якому разі протягом 24 годин після того, як їм це стало відомо про таке.

Якщо існує ймовірність, що порушення безпеки або втрата цілісності можуть негативно вплинути на фізичну або юридичну особу, якій надано довірчу послугу, надавач довірчої послуги також повідомляє без зайвих зволікань фізичну або юридичну особу про порушення безпеки або втрату цілісності.

За доцільності, зокрема якщо порушення безпеки або втрата цілісності стосується двох або більше держав-членів, наглядовий орган, якому надійшло повідомлення, інформує наглядові органи інших відповідних держав-членів та ENISA.

Наглядовий орган, якому надіслано повідомлення, інформує широкий загал або вимагає від надавача довірчих послуг зробити це, якщо він встановить, що розкриття інформації про порушення безпеки або втрати цілісності має суспільний інтерес.

3. Наглядовий орган раз на рік надає ENISA стислий виклад повідомлень про порушення безпеки та втрату цілісності, отриманих від надавачів довірчих послуг.

4. Комісія може шляхом ухвалення імплементаційних актів:

(a) додатково визначити заходи, зазначені в параграфі 1; та

(b) визначити формати і процедури, у тому числі кінцеві терміни, застосовні для цілей параграфа 2.

Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

## *СЕКЦІЯ 3*

## *Кваліфіковані довірчі послуги*

*Стаття 20*

**Нагляд за кваліфікованими надавачами довірчих послуг**

1. Кваліфіковані надавачі довірчих послуг повинні щонайменше кожні 24 місяці за власний кошт проходити аудит з боку органів з оцінювання відповідності. Метою аудиту є підтвердження відповідності кваліфікованих надавачів довірчих послуг та надаваних ними

кваліфікованих довірчих послуг вимогам, установленим у цьому Регламенті. Кваліфіковані надавачі довірчих послуг надають наглядовому органу звіт про оцінювання відповідності протягом трьох робочих днів після його отримання.

2. Без обмеження параграфа 1, наглядовий орган може в будь-який час провести аудит або подати запит до органу з оцінювання відповідності на проведення процедури оцінювання відповідності кваліфікованих надавачів довірчих послуг за їхній власний кошт для підтвердження їх відповідності та відповідності надаваних ними кваліфікованих довірчих послуг вимогам, установленим у цьому Регламенті. Наглядовий орган інформує органи з питань захисту даних про результати аудитів, якщо виявлено порушення правил захисту персональних даних.

3. Якщо наглядовий орган вимагає від кваліфікованого надавача довірчих послуг усунення будь-якого невиконання вимог, установлених у цьому Регламенті, і якщо такий надавач не діє відповідно і, за доцільності, у встановлені наглядовим органом строки, наглядовий орган з урахуванням, зокрема, масштабів, тривалості та наслідків такого невиконання може скасувати статус «кваліфікований» для такого надавача або надаваної ним відповідної послуги та поінформувати зазначений у статті 22(3) орган для цілей оновлення довірчих списків, зазначених у статті 22(1). Наглядовий орган інформує кваліфікованого надавача довірчих послуг про скасування його статусу «кваліфікований» або статусу відповідної послуги «кваліфікована».

4. Комісія може шляхом ухвалення імплементаційних актів установити вихідний номер таких стандартів:

(a) акредитація органів з оцінювання відповідності та для звіту про оцінювання відповідності, зазначеного в параграфі 1;

(b) правила проведення аудиту, за якими органи з оцінювання відповідності оцінюватимуть відповідність кваліфікованих надавачів довірчих послуг, як зазначено в параграфі 1.

Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 21*

**Ініціювання надання кваліфікованої довірчої послуги**

1. Якщо надавачі довірчих послуг, які не мають статусу «кваліфікований», мають намір надавати кваліфіковані довірчі послуги, вони повідомляють наглядовий орган про свій намір та надають звіт про оцінювання відповідності, виданий органом з оцінювання відповідності.

2. Наглядовий орган перевіряє відповідність надавача довірчих послуг та надаваних ним довірчих послуг вимогам цього Регламенту, зокрема вимогам, установленим для кваліфікованих надавачів довірчих послуг та надаваних ними кваліфікованих довірчих послуг.

Якщо наглядовий орган зробить висновок, що надавач довірчих послуг і надавані ним довірчі послуги відповідають вимогам, зазначеним у першому підпараграфі, наглядовий орган надає надавачу довірчих послуг статус «кваліфікований» та повинен поінформувати зазначений у статті 22(3) орган для цілей оновлення довірчих списків, зазначених у статті 22(1), не пізніше ніж через три місяці після повідомлення, зазначеного в параграфі 1 цієї статті.

Якщо перевірку не буде завершено протягом трьох місяців з моменту повідомлення, наглядовий орган інформує надавача довірчих послуг про причини затримки та період, протягом якого перевірку буде завершено.

3. Кваліфіковані надавачі довірчих послуг можуть почати надавати кваліфіковану довірчу послугу після того, як інформацію про статус буде внесено у довірчі списки, зазначені у статті 22(1).

4. Комісія може шляхом ухвалення імплементаційних актів визначити формати і процедури для цілей параграфів 1 і 2. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 22*

**Довірчі списки**

1. Кожна держава-член впроваджує, підтримує в актуальному стані та публікує довірчі списки, у тому числі інформацію про кваліфікованих надавачів довірчих послуг, за які вона є відповідальною, та інформацію, пов'язану з надаваними ними кваліфікованими довірчими послугами.

2. Держави-члени впроваджують, підтримують в актуальному стані та публікують зазначені в параграфі 1 довірчі списки, які скріплено електронним підписом або електронною печаткою, у безпечний спосіб та в формі, що підходить для автоматичного опрацювання.

3. Держави-члени без зайвих зволікань повідомляють Комісії інформацію про орган, відповідальний за впровадження, підтримання в актуальному стані та опублікування національних довірчих списків, та деталі про місця опублікування таких списків, сертифікати, використовувані для скріплення електронним підписом або електронною печаткою довірчих списків, та будь-які зміни, внесені до таких списків.

4. Комісія оприлюднює, з використанням безпечного каналу, інформацію, зазначену в параграфі 3, у скріпленій електронним підписом або електронною печаткою формі, що придатна для автоматизованої обробки.

5. До 18 вересня 2015 року Комісія повинна шляхом ухвалення імплементаційних актів установити зазначену в параграфі 1 інформацію та визначати технічні специфікації і формати для довірчих списків, застосовні для цілей параграфів 1–4. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 23*

**Знак довіри ЄС для кваліфікованих довірчих послуг**

1. Після того, як зазначений у другому підпараграфі статті 21(2) статус «кваліфікований» буде внесено до довірчого списку, зазначеного в статті 22(1), кваліфіковані надавачі довірчих послуг можуть використовувати знак довіри ЄС для позначення в простий, упізнаваний та чіткий спосіб надаваних ними довірчих послуг.

2. Під час використання для кваліфікованих довірчих послуг знаку довіри ЄС, зазначеного в параграфі 1, кваліфіковані надавачі довірчих послуг забезпечують наявність на їхньому сайті посилання на відповідний довірчий список.

3. До 1 липня 2015 року Комісія повинна шляхом ухвалення імплементаційних актів передбачити специфікації щодо форми та, зокрема, представлення, складу, розміру та дизайну знаку довіри ЄС для кваліфікованих довірчих послуг. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 24*

**Вимоги до кваліфікованих надавачів довірчих послуг**

1. Під час видання кваліфікованого сертифіката для довірчої послуги надавач кваліфікованих довірчих послуг за допомогою відповідних засобів та відповідно до національного права перевіряє тотожність та, за доцільності, будь-які конкретні характерні ознаки фізичної або юридичної особи, якій він видає кваліфікований сертифікат.

Кваліфікований надавач довірчих послуг перевіряє інформацію, про яку йдеться в першому абзаці, самостійно або звернувшись до третьої особи відповідно до національного права:

(a) у фізичній присутності фізичної особи або уповноваженого представника юридичної особи; або

(b) дистанційно з використанням засобів електронної ідентифікації, для чого до видання кваліфікованого сертифіката було забезпечено присутність фізичної особи або уповноваженого представника юридичної особи, та з використанням засобів електронної ідентифікації, які відповідають вимогам, установленим у статті 8 щодо рівнів надійності «істотний» або «високий»; або

(c) за допомогою сертифіката кваліфікованого електронного підпису або кваліфікованої електронної печатки, виданого відповідно до пункту (a) чи (b); або

(d) шляхом використання інших методів ідентифікації, які визнано на національному рівні та передбачають надійність, рівнозначну надійності фізичної присутності. Орган з оцінювання відповідності підтверджує рівнозначність надійності.

2. Кваліфікований надавач довірчих послуг, який надає кваліфіковані довірчі послуги, повинен:

(a) інформувати наглядовий орган про будь-які зміни в наданні ним кваліфікованих довірчих послуг, у тому числі про намір припинити свою діяльність;

(b) наймати персонал і, за доцільності, субпідрядників, які мають необхідні знання, надійність, досвід та кваліфікацію та які пройшли відповідну підготовку у сфері безпеки і правил захисту персональних даних, та застосовувати адміністративні й управлінські процедури, які відповідають європейським або міжнародним стандартам;

(c) щодо ризику настання відповідальності за шкоду відповідно до статті 13, володіти достатніми фінансовими ресурсами та/або оформити належне страхування відповідальності згідно з національним правом;

(d) до вступу в договірні відносини повідомляти в прозорий та всебічний спосіб будь-яку особу, яка прагне використовувати кваліфіковану довірчу послугу, про чіткі строки та умови використання такої послуги, у тому числі про будь-які обмеження її використання;

(e) використовувати благонадійні системи і продукти, які захищено від модифікації, та забезпечувати технічну безпеку і надійність підтримуваних ними процесів;

(f) використовувати благонадійні системи для зберігання даних, наданих йому в придатній для перевірки формі так, щоб:

(i) вони були загальнодоступні для пошуку лише за умови отримання згоди особи, з якою пов’язані такі дані,

(ii) тільки уповноважені особи могли вносити записи і зміни до даних, що зберігаються,

(iii) автентичність даних можна було перевірити;

(g) вживати відповідних заходів для запобігання підробленню і викраденню даних;

(h) записувати та зберігати у загальнодоступній формі протягом відповідного періоду, в тому числі після припинення діяльності кваліфікованим надавачем довірчих послуг, усю необхідну інформацію про видані та отримані надавачем кваліфікованих довірчих послуг дані, зокрема, для надання доказів у провадженнях та для забезпечення безперервності надання послуг. Такі записи можна здійснювати в електронній формі;

(i) мати актуальний план припинення діяльності для забезпечення безперервності надання послуг відповідно до положень, що їх перевіряв наглядовий орган згідно з пунктом (i) статті 17(4);

(j) забезпечити законне опрацювання персональних даних відповідно до Директиви 95/46/ЄС;

(k) у разі видання кваліфікованими надавачами довірчих послуг кваліфікованих сертифікатів створити і оновлювати базу даних сертифікатів.

3. Якщо кваліфікований надавач довірчих послуг, який видає кваліфіковані сертифікати, вирішив скасувати сертифікат, він реєструє таке скасування в базі даних сертифікатів та опубліковує статус сертифіката «скасований» вчасно, але в будь-якому разі протягом 24 годин після отримання запиту. Скасування вводять в дію негайно після його опублікування.

4. Щодо параграфа 3, надавачі кваліфікованих довірчих послуг, які видають кваліфіковані сертифікати, надають будь-якій стороні-користувачу інформацію про чинність або скасування виданих ними кваліфікованих сертифікатів. Цю інформацію надають, щонайменше для окремого сертифіката у будь-який час та поза строком чинності сертифіката в автоматичному режимі, який є надійним, безкоштовним і ефективним.

5. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для благонадійних систем і продуктів, які відповідають вимогам, зазначеним у

пунктах (e) і (f) параграфа 2 цієї статті. Припускають, що відповідності вимогам, установленим у цій статті, досягнуто, якщо благонадійні системи та продукти відповідають таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

## *СЕКЦІЯ 4*

## *Юридична сила електронних підписів*

*Стаття 25*

### Юридична сила електронних підписів

1. Електронний підпис не можуть позбавити юридичної сили і можливості бути прийнятим як доказ у провадженнях лише на підставі його електронної форми або його невідповідності вимогам до кваліфікованого електронного підпису.

2. Кваліфікований електронний підпис має таку саму юридичну силу, як власноручний підпис.

3. Кваліфікований електронний підпис на основі кваліфікованого сертифіката, виданого в одній державі-члені, визнають кваліфікованим електронним підписом у всіх інших державах-членах.

*Стаття 26*

### Вимоги до удосконалених електронних підписів

Удосконалений електронний підпис повинен відповідати таким вимогам:

(a) він повинен бути однозначно пов’заний з підписувачем;

(b) він повинен надавати можливість ідентифікувати підписувача;

(c) його необхідно створювати з використанням даних для створення електронного підпису, які підписувач може з високим ступенем упевненості використовувати лише під своїм одноосібним контролем;

(d) він повинен бути зв’язаний зі скріпленими ним даними у такий спосіб, щоб можна було виявити будь-яку подальшу зміну даних.

*Стаття 27*

### Електронні підписи в публічних послугах

1. Якщо державі-члену потрібен удосконалений електронний підпис для використання онлайн-послуг, які пропонує орган публічного сектора або які пропонують від його імені, така держава-член визнає вдосконалені електронні підписи, вдосконалені електронні підписи на основі кваліфікованого сертифіката електронних підписів та кваліфіковані електронні підписи щонайменше в форматах або з використанням методів, які визначено в імплементаційних актах, про які йдеться в параграфі 5.

2. Якщо державі-члену потрібен удосконалений електронний підпис на підставі кваліфікованого сертифіката для використання онлайн-послуг, які пропонує орган публічного сектора або які пропонують від його імені, така держава-член визнає вдосконалені електронні підписи на основі кваліфікованого сертифіката та кваліфіковані електронні підписи щонайменше в форматах або з використанням методів, які визначено в імплементаційних актах, про які йдеться в параграфі 5.

3. Держави-члени не повинні подавати запит для транскордонного використання в онлайн-послугах, які пропонує орган публічного сектора, на електронний підпис з вищим рівнем безпеки, ніж кваліфікований електронний підпис.

4. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для вдосконалених електронних підписів. Припускають, що відповідності вимогам до вдосконалених електронних підписів, зазначених в параграфах 1 і 2 цієї статті та в статті 26,

досягнуто, якщо вдосконалений електронний підпис відповідає таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

5. До 18 вересня 2015 року з урахуванням чинних практик, стандартів та правових актів Союзу Комісія повинна ухвалити імплементаційні акти, у яких визначено референтні формати вдосконалених електронних підписів або референтні методи, якщо використовують альтернативні формати. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 28*

**Кваліфіковані сертифікати електронних підписів**

1. Кваліфіковані сертифікати електронних підписів повинні відповідати вимогам, установленим у додатку I.

2. На кваліфіковані сертифікати електронних підписів не поширюються будь-які обов'язкові вимоги, що виходять за межі вимог, установлених у додатку I.

3. Кваліфіковані сертифікати електронних підписів можуть мати необов'язкові додаткові конкретні характерні ознаки. Такі характерні ознаки не повинні впливати на інтероперабельність і визнання кваліфікованих електронних підписів.

4. Якщо кваліфікований сертифікат електронних підписів скасовано після початкової активації, він втрачає свою чинність з моменту його скасування і його статус за жодних обставин не повинен бути поновленим.

5. Держави-члени можуть установити національні правила щодо призупинення чинності кваліфікованих сертифікатів електронного підпису відповідно до таких умов:

(a) якщо чинність кваліфікованого сертифіката електронного підпису призупинено, такий сертифікат втрачає свою чинність на період такого призупинення;

(b) строк призупинення чітко зазначають у базі даних сертифікатів, а статус «призупинений» повинен бути видимим протягом періоду призупинення в службі, яка надає інформацію про статус сертифіката.

6. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для кваліфікованих сертифікатів електронного підпису. Припускають, що відповідності вимогам, установленим у додатку I, досягнуто, якщо кваліфікований сертифікат електронного підпису відповідає таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 29*

**Вимоги до засобів для створення кваліфікованого електронного підпису**

1. Засоби для створення кваліфікованого електронного підпису повинні відповідати вимогам, установленим у додатку II.

2. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для засобів для створення кваліфікованого електронного підпису. Припускають, що відповідності вимогам, установленим у додатку II, досягнуто, якщо засіб для створення кваліфікованого електронного підпису відповідає таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 30*

**Сертифікація засобів для створення кваліфікованого електронного підпису**

1. Відповідні публічні або приватні органи, що їх призначила держава-член, здійснюють сертифікацію відповідності засобів для створення кваліфікованого електронного підпису вимогам додатку II.

2. Держави-члени повідомляють Комісії назви та адреси публічного або приватного органу, зазначеного у параграфі 1. Комісія надає таку інформацію державам-членам.

3. Зазначена в параграфі 1 сертифікація повинна ґрунтуватися на одному з таких процесів:

(a) на процесі оцінювання безпеки, здійснюваному відповідно до одного зі стандартів оцінювання безпеки продуктів інформаційних технологій, що входять у список, створений відповідно до другого підпараграфа, або

(b) на процесі, відмінному від процесу, зазначеного в пункті (a), за умови, що у ньому використовують зіставні рівні безпеки, та за умови, що публічний або приватний орган, зазначений у параграфі 1, повідомляє про цей процес Комісію. Такий процес можуть використати лише за відсутності зазначених в пункті (a) стандартів або під час зазначеного в пункті (a) процесу оцінювання безпеки.

Комісія шляхом ухвалення імплементаційних актів створює список стандартів для оцінювання безпеки продуктів інформаційних технологій, зазначених у пункті (a). Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

4. Комісію необхідно наділити повноваженням ухвалювати делеговані акти відповідно до статті 47 щодо встановлення конкретних критеріїв, яким повинні відповідати призначені органи, про які йдеться в параграфі 1 цієї статті.

*Стаття 31*

**Публікація списку сертифікованих засобів для створення кваліфікованого електронного підпису**

1. Держави-члени повідомляють Комісії без зайвих зволікань та не пізніше ніж через один місяць після завершення сертифікації інформацію про засоби для створення кваліфікованого електронного підпису, що їх сертифікували органи, зазначені в статті 30(1). Вони також повідомляють Комісії без зайвих зволікань та не пізніше ніж через один місяць після скасування сертифікації інформацію про засоби для створення електронного підпису, які більше не є сертифікованими.

2. На основі отриманої інформації Комісія створює, опубліковує та веде список сертифікованих засобів для створення кваліфікованого електронного підпису.

3. Комісія може шляхом ухвалення імплементаційних актів визначити формати і процедури, застосовні для досягнення зазначеної у параграфі 1 цілі. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 32*

**Вимоги до валідації кваліфікованих електронних підписів**

1. Процес валідації кваліфікованого електронного підпису підтверджує чинність електронного підпису за умови, що:

(a) сертифікат, який підтримує підпис, на момент підписання був кваліфікованим сертифікатом електронного підпису та відповідав вимогам, установленим у додатку I;

(b) кваліфікований сертифікат видано кваліфікованим надавачем довірчих послуг і був дійсним на момент підписання;

(c) дані для валідації підпису відповідають даним, що їх надали стороні-користувачу;

(d) унікальний набір даних, що представляє підписувача в сертифікаті, правильно надали стороні-користувачу;

(e) стороні-користувачу чітко повідомили про використання будь-якого псевдоніма, якщо такий використали під час підписання;

(f) електронний підпис створено засобом для створення кваліфікованого електронного підпису;

(g) цілісність підписаних даних не скомпрометовано;

(h) на момент підписання виконано вимоги, передбачені у статті 26.

2. Система, яку використовують для валідації електронного підпису, повинна надавати стороні-користувачу правильний результат процесу валідації та надавати стороні-користувачу змогу

виявити будь-які проблеми, пов’язані з безпекою.

3. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для валідації кваліфікованого електронного підпису. Припускають, що відповідності вимогам, установленим у параграфі 1, досягнуто, якщо валідація кваліфікованих електронних підписів відповідає таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 33*

**Кваліфікована послуга валідації кваліфікованих електронних підписів**

1. Кваліфіковану послугу валідації кваліфікованих електронних підписів може надавати лише кваліфікований надавач довірчих послуг, який:

(a) здійснює валідацію відповідно до статті 32(1) та

(b) дає сторонам-користувачам змогу отримувати результати процесу валідації в автоматичному режимі, який є надійним, ефективним та використовує вдосконалений електронний підпис або вдосконалену електронну печатку надавача кваліфікованої послуги перевірки.

2. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для кваліфікованих послуг валідації, зазначених у параграфі 1. Припускають, що відповідності вимогам, установленим у параграфі 1, досягнуто, якщо послуга валідації кваліфікованого електронного підпису відповідає таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 34*

**Кваліфікована послуга зберігання кваліфікованих електронних підписів**

1. Кваліфіковану послугу зберігання кваліфікованих електронних підписів може надавати лише кваліфікований надавач довірчих послуг, який використовує процедури і технології, що можуть подовжувати благонадійність кваліфікованого електронного підпису поза межі технологічного строку чинності.

2. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для кваліфікованої послуги зберігання кваліфікованих електронних підписів. Презюмується, що відповідності вимогам, установленим у параграфі 1, досягнуто, якщо заходи з надання послуги валідації кваліфікованого електронного підпису відповідають таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

## *СЕКЦІЯ 5*

## *Електронні печатки*

*Стаття 35*

**Юридична сила електронної печатки**

1. Електронну печатку не можуть позбавити юридичної сили і можливості бути прийнятою як доказ у провадженнях лише на підставі її електронної форми або її невідповідності вимогам до кваліфікованої електронної печатки.

2. Кваліфікована електронна печатка користується презумпцією цілісності даних і правильності походження таких даних, з якими кваліфікована електронна печатка пов’язана.

3. Кваліфіковану електронну печатку на основі кваліфікованого сертифіката, виданого в одній державі-члені, визнають кваліфікованою електронною печаткою у всіх інших держав-членів.

*Стаття 36*

**Вимоги до удосконалених електронних печаток**

Удосконалена електронна печатка повинна відповідати таким вимогам:

(a) вона повинна бути однозначно пов’язаною зі створювачем печатки;

(b) вона повинна надавати можливість ідентифікувати створювача печатки;

(c) її необхідно створювати з використанням даних для створення електронної печатки, які створювач печатки може з високим ступенем упевненості та під своїм контролем використовувати для створення електронної печатки, і

(d) вона повинна бути зв’язаною з даними, з якими вона пов’язана, у такий спосіб, щоб можна було виявити будь-яку подальшу зміну даних.

*Стаття 37*

**Електронні печатки в публічних послугах**

1. Якщо державі-члену потрібна вдосконалена електронна печатка для використання онлайн-послуг, які пропонує орган публічного сектора або які пропонують від його імені, така держава-член визнає вдосконалені електронні печатки, вдосконалені електронні печатки на основі кваліфікованого сертифіката електронних печаток та кваліфіковані електронні печатки щонайменше в форматах або з використанням методів, про які йдеться в параграфі 5.

2. Якщо державі-члену потрібна вдосконалена електронна печатка на основі кваліфікованого сертифіката для використання онлайн-послуг, які пропонує орган публічного сектора або які пропонують від його імені, така держава-член визнає вдосконалені електронні печатки на основі кваліфікованого сертифіката та кваліфіковані електронні печатки принаймні в форматах або з використанням методів, про які йдеться в параграфі 5.

3. Держави-члени не повинні подавати запит для транскордонного використання в онлайн-послугах, які пропонує орган публічного сектора, на електронні печатки з вищим рівнем безпеки, ніж кваліфіковані електронні печатки.

4. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для вдосконалених електронних печаток. Припускають, що відповідності вимог до вдосконалених електронних печаток, зазначених в параграфах 1 і 2 цієї статті та в статті 36, досягнуто, якщо вдосконалена електронна печатка відповідає таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

5. До 18 вересня 2015 року з урахуванням чинних практик, стандартів та правових актів Союзу Комісія повинна ухвалити імплементаційні акти, у яких визначено референтні формати вдосконалених електронних печаток або референтні методи, якщо використовують альтернативні формати. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 38*

**Кваліфіковані сертифікати електронних печаток**

1. Кваліфіковані сертифікати електронних печаток повинні відповідати вимогам, установленим у додатку III.

2. На кваліфіковані сертифікати електронних печаток не поширюються будь-які обов’язкові вимоги, що виходять за межі вимог, установлених у додатку III.

3. Кваліфіковані сертифікати електронних печаток можуть мати необов’язкові додаткові конкретні характерні ознаки. Такі характерні ознаки не повинні впливати на інтероперабельність і визнання кваліфікованих електронних печаток.

4. Якщо кваліфікований сертифікат електронних печаток скасовано після початкової активації, він втрачає свою чинність з моменту його скасування і його статус за жодних обставин не повинен бути поновленим.

5. Держави-члени можуть установити національні правила щодо призупинення чинності кваліфікованих сертифікатів електронної печатки відповідно до таких умов:

(a) якщо чинність кваліфікованого сертифіката електронної печатки призупинено, такий сертифікат втрачає свою чинність на період такого призупинення;

(b) строк призупинення чітко зазначають у базі даних сертифікатів, а статус «призупинений» повинен бути видимим протягом періоду призупинення в службі, яка надає інформацію про статус сертифіката.

6. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для кваліфікованих сертифікатів електронних печаток. Припускають, що відповідності вимог, установлених у додатку III, досягнуто, якщо кваліфікований сертифікат електронної печатки відповідає таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

*Стаття 39*

**Засоби для створення кваліфікованої електронної печатки**

1. Статтю 29 застосовують mutatis mutandis до вимог до засобів для створення кваліфікованої електронної печатки.

2. Статтю 30 застосовують mutatis mutandis до сертифікації засобів для створення кваліфікованої електронної печатки.

3. Статтю 31 застосовують mutatis mutandis до публікації списку сертифікованих засобів для створення кваліфікованої електронної печатки.

*Стаття 40*

**Валідація та зберігання кваліфікованих електронних печаток**

Статті 32, 33 і 34 застосовують mutatis mutandis до валідації та зберігання кваліфікованих електронних печаток.

## *СЕКЦІЯ 6*

## *Юридична сила електронних позначок часу*

*Стаття 41*

**Юридична сила електронних позначок часу**

1. Електронну позначку часу не можуть позбавити юридичної сили і можливості бути прийнятою як доказ у провадженнях лише на підставі її електронної форми або її невідповідності вимогам до кваліфікованої позначки часу.

2. Кваліфікована електронна позначка часу має презумпцію точності дати і часу, на які вона вказує, та цілісності даних, з якими такі дата та час пов’язані.

3. Кваліфіковану електронну позначку часу, випущену в одній з держав-членів, визнають кваліфікованою електронною позначкою часу у всіх інших державах-членах.

*Стаття 42*

**Вимоги до кваліфікованих позначок часу**

1. Кваліфікована позначка часу повинна відповідати таким вимогам:

(a) вона повинна встановити зв’язок дати і часу з даними в такий спосіб, щоб розумно виключити можливість невиявної зміни даних;

(b) вона повинна ґрунтуватися на точному джерелі часу, синхронізованому з Всесвітнім координованим часом (UTC);

(c) вона повинна бути скріплена вдосконаленим електронним підписом або вдосконаленою електронною печаткою кваліфікованого надавача довірчих послуг або з використанням іншого рівнозначного методу.

2. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для встановлення зв'язку дати та часу з даними та для точного джерела часу. Припускають, що відповідності вимогам, установленим у параграфі 1, досягнуто, якщо прив'язання дати та часу до даних та точне джерело часу відповідають таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

## *СЕКЦІЯ 7*

## *Послуги реєстрованої електронної доставки*

*Стаття 43*

### Юридична сила послуги реєстрованої електронної доставки

1. Дані, які відправляють та отримують шляхом використання послуги реєстрованої електронної доставки, не можуть позбавити юридичної сили і можливості бути прийнятими як доказ у провадженнях лише на підставі їх електронної форми або їх невідповідності вимогам до кваліфікованої послуги реєстрованої електронної доставки.

2. Дані, які відправляють та отримують шляхом використання кваліфікованої послуги реєстрованої електронної доставки, користуються презумпцією цілісності даних, доставка таких даних ідентифікованим відправником, отримання ідентифікованим отримувачем та точності дати і часу відправлення та отримання, які зазначають під час надання кваліфікованої послуги реєстрованої електронної доставки.

*Стаття 44*

### Вимоги до кваліфікованої послуги реєстрованої електронної доставки

1. Кваліфіковані послуги реєстрованої електронної доставки повинні відповідати таким вимогам:

(a) їх повинні надавати один чи декілька кваліфікованих надавачів довірчих послуг;

(b) вони повинні забезпечувати ідентифікацію відправника з високим рівнем довіри;

(c) вони повинні забезпечувати ідентифікацію отримувача перед доставленням даних;

(d) відправлення та отримання даних повинні бути захищеними вдосконаленим електронним підписом або вдосконаленою електронною печаткою кваліфікованого надавача довірчих послуг у спосіб, який виключає можливість невиявної зміни даних;

(e) відправника й отримувача даних необхідно чітко повідомити про будь-яку зміну даних, необхідну для відправлення або отримання даних;

(f) дату і час відправлення, отримання та будь-якої зміни даних необхідно позначити за допомогою кваліфікованої електронної позначки часу;

У разі передання даних між двома або більше кваліфікованими надавачами довірчих послуг вимоги пунктів (a)–(f) застосовують до всіх кваліфікованих надавачів довірчих послуг.

2. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для процесів відправлення та отримання даних. Припускають, що відповідності вимогам, установленим у параграфі 1, досягнуто, якщо процеси відправлення та отримання даних відповідають таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

## *СЕКЦІЯ 8*

## *Автентифікація веб-сайту*

*Стаття 45*

### Вимоги до кваліфікованих сертифікатів автентифікації веб-сайту

1. Кваліфіковані сертифікати автентифікації веб-сайту повинні відповідати вимогам, установленим у додатку IV.

2. Комісія може шляхом ухвалення імплементаційних актів установити вихідні номери стандартів для кваліфікованих сертифікатів автентифікації веб-сайту. Припускають, що відповідності вимогам, установленим у додатку IV, досягнуто, якщо кваліфікований сертифікат автентифікації веб-сайту відповідає таким стандартам. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, зазначеної в статті 48(2).

## ГЛАВА IV
## ЕЛЕКТРОННІ ДОКУМЕНТИ

*Стаття 46*

**Юридична сила електронних документів**

Електронний документ не можуть позбавити юридичної сили і можливості бути прийнятим як доказ у провадженнях лише на підставі його електронної форми.

## ГЛАВА V
## ДЕЛЕГУВАННЯ ПОВНОВАЖЕНЬ ТА ІМПЛЕМЕНТАЦІЙНІ ПОЛОЖЕННЯ

*Стаття 47*

**Процедура делегування**

1. Повноваження ухвалювати делеговані акти покладають на Комісію відповідно до умов, визначених у цій статті.

2. Повноваження ухвалювати делеговані акти, зазначені в статті 30(4), покладають на Комісію на невизначений строк, починаючи з 17 вересня 2014 року.

3. Делеговані повноваження, зазначені в статті 30(4), може бути скасовано в будь-який час Європейським Парламентом або Радою. У разі ухвалення рішення про відкликання, делеговане повноваження, зазначене у такому рішенні, анулюється. Воно набуває чинності наступного дня після публікації рішення в *Офіційному віснику Європейського Союзу* або із вказаної в ньому дати. Воно не впливає на чинність будь-яких делегованих актів, що вже набули чинності.

4. Відразу після ухвалення делегованого акту, Комісія повідомляє про це одночасно Європейський Парламент і Раду.

5. Делегований акт, ухвалений відповідно до статті 30(4), набуває чинності, лише якщо з боку Європейського Парламенту чи Ради впродовж двох місяців з дати повідомлення Європейського Парламенту й Ради про цей акт, не було висловлено жодних заперечень, або якщо ще до закінчення цього періоду і Європейський Парламент, і Рада повідомили Комісії, що вони не заперечуватимуть. Такий період подовжують на два місяці за ініціативи Європейського Парламенту або Ради.

*Стаття 48*

**Процедура комітету**

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

2. У разі покликання на цей параграф застосовують статтю 5 Регламенту (ЄС) № 182/2011.

## ГЛАВА VI
## ПРИКІНЦЕВІ ПОЛОЖЕННЯ

*Стаття 49*

**Перегляд**

Комісія повинна здійснити перегляд застосування цього Регламенту та надати звіт Європейському Парламенту та Раді до 1 липня 2020 року. Комісія оцінює, зокрема, чи доцільно змінювати сферу застосування цього Регламенту або його конкретних положень, у тому числі статтю 6, пункт (f) статті 7 та статті 34, 43, 44 і 45, враховуючи досвід, здобутий під час застосування цього Регламенту, а також технологічні, ринкові і правові досягнення.

До звіту, зазначеного в першому параграфі, додають, за доцільності, законодавчі пропозиції.

Крім того, Комісія кожні 4 роки після надання звіту, зазначеного в першому параграфі, надає Європейському Парламенту і Раді звіт про прогрес у досягненні цілей цього Регламенту.

*Стаття 50*

**Скасування**

1. Директиву 1999/93/ЄС скасувати з 1 липня 2016 року.

2. Поклилання на скасовану Директиву необхідно тлумачити як покликання на цей Регламент.

*Стаття 51*

**Перехідні заходи**

1. Безпечні засоби для створення підпису, відповідність яких встановлено відповідно до статті 3(4) Директиви 1999/93/ЄС, вважають засобами для створення кваліфікованого підпису за цим Регламентом.

2. Кваліфіковані сертифікати, видані фізичним особам за Директивою 1999/93/ЄС, вважають кваліфікованими сертифікатами електронних підписів за цим Регламентом до закінчення строку їх чинності.

3. Надавач послуг сертифікації, який видає кваліфіковані сертифікати за Директивою 1999/93/ЄС, надає звіт про оцінювання відповідності наглядовому органу якнайшвидше, але не пізніше ніж 1 липня 2017 року. До надання такого звіту з оцінювання відповідності та завершення оцінювання наглядовим органом такого надавача послуг сертифікації, останнього вважають кваліфікованим надавачем довірчих послуг за цим Регламентом.

4. Якщо надавач послуг сертифікації, який видає кваліфіковані сертифікати за Директивою 1999/93/ЄС, не надасть звіт про оцінювання відповідності наглядовому органу протягом строку, зазначеного в параграфі 3, такого надавача послуг сертифікації не вважатимуть кваліфікованим надавачем довірчих послуг за цим Регламентом з 2 липня 2017 року.

*Стаття 52*

**Набуття чинності**

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

2. Цей Регламент застосовують з 1 липня 2016 року, за винятком такого:

(a) статті 8(3), 9(5), 12(2)–(9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) і (5), 28(6), 29(2), 30(3) і (4), 31(3), 32(3), 33(2), 34(2), 37(4) і (5), 38(6), 42(2), 44(2), 45(2), статті 47 і 48 застосовують з 17 вересня 2014 року;

(b) статтю 7, статтю 8(1) і (2), статті 9, 10, 11 та статтю 12(1) застосовують з дати застосування імплементаційних актів, зазначених у статтях 8(3) і 12(8);

(c) статтю 6 застосовують через 3 роки з дати застосування імплементаційних актів, зазначених у статтях 8(3) і 12(8).

3. Якщо нотифіковану схему електронної ідентифікації внесено у список, що його опублікувала Комісія відповідно до статті 9, до дати, зазначеної в пункті (c) параграфа 2 цієї статті, визнання

засобів електронної ідентифікації за цією схемою відповідно до статті 6 необхідно здійснити не пізніше ніж через 12 місяців після опублікування цієї схеми, але не раніше ніж у день, зазначений у пункті (c) параграфа 2 цієї статті.

4. Незважаючи на пункт (c) параграфа 2 цієї статті, держава-член може вирішити, що засоби електронної ідентифікації за схемою електронної ідентифікації, що її нотифікувала відповідно до статті 9(1) інша держава-член, визнає перша держава-член з дати застосування імплементаційних актів, зазначених у статтях 8(3) і 12(8). Відповідні держави-члени повідомляють про це Комісію. Комісія оприлюднює таку інформацію.

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

Учинено в Брюсселі 23 липня 2014 року.

*За Парламент*
*Президент*
M. SCHULZ
*За Раду*
*Президент*
S. GOZI

---

(1) ОВ C 351, 15.11.2012, с. 73.

(2) Позиція Європейського Парламенту від 3 квітня 2014 року (ще не опубліковано в Офіційному віснику) та Рішення Ради від 23 липня 2014 року.

(3) Директива Європейського Парламенту і Ради 1999/93/ЄС від 13 грудня 1999 року про рамки Співтовариства для електронних підписів (ОВ L 13, 19.01.2000, с. 12).

(4) ОВ C 50 E, 21.02.2012, с. 1.

(5) Директива 2006/123/ЄС Європейського Парламенту і Ради від 12 грудня 2006 року про послуги на внутрішньому ринку (ОВ L 376, 27.12.2006, с. 36).

(6) Директива 2011/24/ЄС Європейського Парламенту і Ради від 9 березня 2011 року про застосування прав пацієнтів у межах транскордонного медичного обслуговування (ОВ L 88, 04.04.2011, с. 45).

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

(8) Рішення Ради 2010/48/ЄС від 26 листопада 2009 року щодо укладення Європейським Співтовариством Конвенції ООН про права осіб з інвалідністю (ОВ L 23, 27.01.2010, с. 35).

(9) Регламент Європейського Парламенту і Ради (ЄС) № 765/2008 від 9 липня 2008 року про встановлення вимог до акредитації та ринкового нагляду у зв'язку з реалізацією продуктів та про скасування Регламенту (ЄЕС) № 339/93 (ОВ L 218, 13.08.2008, с. 30).

(10) Рішення Комісії 2009/767/ЄС від 16 жовтня 2009 року про встановлення заходів, що сприяють використанню процедур за допомогою електронних засобів через єдині пункти зв'язку відповідно до Директиви Європейського Парламенту і Ради 2006/123/ЄС про послуги на внутрішньому ринку (ОВ L 274, 20.10.2009, с. 36).

(11) Рішення Комісії 2011/130/ЄС від 25 лютого 2011 року про встановлення мінімальних вимог для транскордонного опрацювання документів, що їх підписали електронно компетентні органи за Директивою 2006/123/ЄС Європейського Парламенту і Ради про послуги на внутрішньому ринку (ОВ L 53, 26.02.2011, с. 66).

(12) Регламент Європейського Парламенту і Ради (ЄС) № 182/2011 від 16 лютого 2011 року про встановлення загальних норм та принципів щодо механізмів контролю державами-членами здійснення Комісією виконавчих повноважень (ОВ L 55, 28.02.2011, с. 13).

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

(14) ОВ C 28, 30.01.2013, с. 6.

(15) Директива Європейського Парламенту і Ради 2014/24/ЄС від 26 лютого 2014 року про публічні закупівлі та про скасування Директиви 2004/18/ЄС (ОВ L 94, 28.03.2014, с. 65).

---

## ДОДАТОК I

## ВИМОГИ ДО КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ЕЛЕКТРОННИХ ПІДПИСІВ

Кваліфіковані сертифікати електронного підпису повинні містити:

(a) зазначення, щонайменше в формі, придатній для автоматизованої обробки, того, що сертифікат видано як кваліфікований сертифікат електронного підпису;

(b) набір даних, що однозначно представляють кваліфікованого надавача довірчих послуг, який видає кваліфіковані сертифікати, і містять щонайменше назву держави-члена, у якій засновано такого надавача, та:

— для юридичної особи: найменування та, за доцільності, реєстраційний номер, як зазначено в офіційних записах,

— для фізичної особи: прізвище та ім’я особи;

(c) щонайменше прізвище та ім’я підписувача або псевдонім; якщо використовують псевдонім, це необхідно чітко вказати;

(d) дані для валідації електронного підпису, які відповідають даним для створення електронного підпису;

(e) детальну інформацію про початок та завершення строку чинності сертифіката;

(f) ідентифікаційний код сертифіката, що повинен бути унікальним для кваліфікованого надавача довірчих послуг;

(g) удосконалений електронний підпис або удосконалену електронну печатку кваліфікованого надавача довірчих послуг, який видає сертифікат;

(h) місце, де безоплатно надають сертифікат, який підтримує удосконалений електронний підпис або удосконалену електронну печатку, зазначені в пункті (g);

(i) місце надання послуг, які можна використати для подання запиту на перевірку статусу чинності кваліфікованого сертифіката;

(j) якщо дані для створення електронного підпису, пов’язані з даними для валідації електронного підпису, знаходяться в засобах для створення кваліфікованого електронного підпису, належне зазначення цього щонайменше в формі, придатній для автоматизованої обробки.

## ДОДАТОК II

## ВИМОГИ ДО ЗАСОБІВ ДЛЯ СТВОРЕННЯ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ

1. Засоби для створення кваліфікованого електронного підпису повинні забезпечувати за допомогою належних технічних та процедурних засобів та процедур щонайменше:

   (a) у розумних межах конфіденційність даних для створення електронного підпису, використовуваних для створення електронного підпису;

   (b) лише одноразове внесення даних для створення електронного підпису, використовуваних для створення електронного підпису;

   (c) унеможливлення, з надійністю розумного ступеня, отримання даних для створення електронного підпису, використовуваних для створення електронного підпису, та надійний захист електронного підпису від підроблення шляхом використання наявних технологій;

   (d) надійний захист законним підписувачем даних для створення електронного підпису, використовуваних для створення електронного підпису, від використання іншими особами.

2. Засоби для створення кваліфікованого електронного підпису не повинні змінювати дані, які необхідно підписати, та не повинні запобігати представленню таких даних підписувачу до підписання.

3. Генерування даних для створення електронного підпису та управління ними від імені

підписувача можуть здійснювати лише кваліфіковані надавачі довірчих послуг.

4. Без обмеження пункту (d) пункту 1, кваліфіковані надавачі довірчих послуг, які управляють даними для створення електронного підпису від імені підписувача, можуть дублювати дані для створення електронного підпису лише для цілей створення резервної копії за умови дотримання таких вимог:

   (a) рівень безпеки продубльованих наборів даних повинен бути таким самим, як рівень безпеки оригінальних наборів даних;

   (b) кількість продубльованих наборів даних не повинна перевищувати мінімальну кількість, необхідну для забезпечення безперервності надання послуги.

## ДОДАТОК III

## ВИМОГИ ДО КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ЕЛЕКТРОННИХ ПЕЧАТОК

Кваліфіковані сертифікати електронних печаток повинні містити:

(a) зазначення, щонайменше в формі, придатній для автоматизованої обробки, того, що сертифікат видано як кваліфікований сертифікат електронної печатки;

(b) набір даних, що однозначно представляють кваліфікованого надавача довірчих послуг, який видає кваліфіковані сертифікати, і містять щонайменше назву держави-члена, у якій його засновано такого надавача, та:

   — для юридичної особи: найменування та, за доцільності, реєстраційний номер, як зазначено в офіційних записах,

   — для фізичної особи: прізвище та ім’я особи;

(c) щонайменше найменування створювача печатки та, за доцільності, реєстраційний номер, як зазначено в офіційних записах;

(d) дані для валідації електронної печатки, які відповідають даним для створення електронної печатки;

(e) детальну інформацію про початок та завершення строку чинності сертифіката;

(f) ідентифікаційний код сертифіката, що повинен бути унікальним для кваліфікованого надавача довірчих послуг;

(g) удосконалений електронний підпис або удосконалену електронну печатку кваліфікованого надавача довірчих послуг, який видає сертифікат;

(h) місце, де безоплатно надають сертифікат, який підтримує удосконалений електронний підпис або удосконалену електронну печатку, зазначені в пункті (g);

(i) місце надання послуг, які можна використати для подання запиту на перевірку статусу чинності кваліфікованого сертифіката;

(j) якщо дані для створення електронної печатки, пов’язані з даними для валідації електронної печатки, знаходяться в засобах для створення кваліфікованої електронної печатки, належне зазначення цього щонайменше в формі, придатній для автоматизованої обробки.

## ДОДАТОК IV

## ВИМОГИ ДО КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ АВТЕНТИФІКАЦІЇ ВЕБ-САЙТУ

Кваліфіковані сертифікати автентифікації веб-сайту повинні містити:

(a) зазначення, щонайменше в формі, придатній для автоматизованої обробки, того, що сертифікат видано як кваліфікований сертифікат автентифікації веб-сайту;

(b) набір даних, що однозначно представляють кваліфікованого надавача довірчих послуг, який видає кваліфіковані сертифікати, і містять щонайменше назву держави-члена, у якій його засновано такого надавача, та:

— для юридичної особи: найменування та, за доцільності, реєстраційний номер, як зазначено в офіційних записах,

— для фізичної особи: прізвище та ім’я особи;

(c) для фізичних осіб: щонайменше прізвище та ім’я або псевдонім особи, якій видано сертифікат. Якщо використовують псевдонім, це необхідно чітко вказати;

для юридичних осіб: щонайменше найменування юридичної особи, якій видано сертифікат, та, за доцільності, реєстраційний номер, як зазначено в офіційних записах;

(d) складові адреси, у тому числі щонайменше місто та державу фізичної або юридичної особи, якій видано сертифікат, та, за доцільності, як зазначено в офіційних записах;

(e) назву домену, використовуваного фізичною або юридичною особою, якій видано сертифікат;

(f) детальну інформацію про початок та завершення строку чинності сертифіката;

(g) ідентифікаційний код сертифіката, що повинен бути унікальним для кваліфікованого надавача довірчих послуг;

(h) удосконалений електронний підпис або удосконалену електронну печатку кваліфікованого надавача довірчих послуг, який видає сертифікат;

(i) місце, де безоплатно надають сертифікат, який підтримує удосконалений електронний підпис або удосконалену електронну печатку, зазначені в пункті (h);

(j) місце надання послуг щодо статусу чинності сертифіката, які можна використати для подання запиту на перевірку статусу чинності кваліфікованого сертифіката.