

РЕГЛАМЕНТ (ЄС) № 910/2014 ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ ТА РАДИ**від 23 липня 2014 року**

про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ ТА РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

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

Беручи до уваги пропозицію Європейської Комісії,

Після передачі проекту законодавчого акта до національних парламентів,

Беручи до уваги висновок Європейського економічного та соціального комітету⁽¹⁾,

Діючи відповідно до звичайної законодавчої процедури⁽²⁾,

Оскільки:

- (1) Побудова довіри в он-лайн середовищі є ключовим завданням для економічного та соціального розвитку. Відсутність довіри, зокрема, через передбачувану відсутність правової визначеності, змушує споживачів, бізнес та адміністрації коливатися при здійсненні транзакцій в електронному вигляді та впроваджувати нові послуги.
- (2) Цей Регламент спрямований на підвищення рівня довіри до електронних транзакцій на внутрішньому ринку шляхом надання загальної основи для безпечної електронної взаємодії між підприємствами, громадянами і державними органами, тим самим підвищуючи ефективність державних і приватних он-лайн послуг, електронного бізнесу та електронної торгівлі в ЄС.
- (3) Директива 1999/93/ЄС Європейського Парламенту та Ради ⁽³⁾ стосується електронних підписів без надання всебічних транскордонних та міжгалузевих основ для безпечних, надійних і простих у використанні електронних транзакцій. Цей Регламент удосконалює та розширює напрацьоване законодавство, що представляє зазначена Директива.
- (4) Прийнятий Комісією 26 серпня 2013 року «Цифровий порядок денний Європи» визначив фрагментацію цифрового ринку, відсутність сумісності і зростання кіберзлочинності як основні перешкоди на шляху ефективного розвитку цифрової економіки. У своєму звіті 2010 року про громадянство Європейського Союзу, що має назву “Ліквідація перешкод у реалізації прав громадян ЄС”, Комісія також наголосила на необхідності вирішення основних проблем, які заважають громадянам ЄС користуватися перевагами єдиного цифрового ринку і транскордонних цифрових послуг.
- (5) У своїх висновках від 4 лютого 2011 року та від 23 жовтня 2011 року Європейська Рада закликала Комісію створити єдиний цифровий ринок до 2015 року, щоб домогтися швидкого прогресу у ключових областях цифрової економіки та сприяти запровадженню єдиного повністю інтегрованого цифрового ринку шляхом полегшення транскордонного використання он-лайн послуг, зокрема використання безпечних електронної ідентифікації та автентифікації.

⁽¹⁾ ОВ С 351 від 15.11.2012, С. 73.

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

⁽³⁾ Директива Європейського Парламенту та Ради 1999/93/ЄС від 13 грудня 1999 року про політику Європейського Співтовариства щодо електронних підписів (ОВ L 13 від 19.1.2000, С. 12).

- (6) У своїх висновках від 27 травня 2011 року Рада закликала Комісію сприяти запровадженню єдиного цифрового ринку шляхом створення належних умов для взаємного транскордонного визнання ключових компонентів, таких як електронна ідентифікація, електронні документи, електронні підписи та електронні послуги доставки, а також для врегулювання технічно сумісних послуг електронного управління по всій території Європейського Союзу.
- (7) Європейський Парламент у своїй Резолюції від 21 вересня 2010 року про завершення формування внутрішнього ринку, що стосується електронної торгівлі ⁽¹⁾ підкреслив важливість забезпечення безпеки електронних послуг, зокрема електронних підписів, а також необхідність створення інфраструктури відкритого ключа на загально європейському рівні, і закликав Комісію створити портал між європейськими органами перевірки для забезпечення транскордонної сумісності електронних підписів та підвищення рівня безпеки транзакцій, що здійснюється з використанням Інтернету.
- (8) Директива 2006/123/ЄС Європейського Парламенту та Ради ⁽²⁾ вимагає від держав-членів створення єдиного інформаційно-розрахункового центру для того, щоб всі процедури і формальності, пов'язані з доступом до послуг та їх здійсненням могли здійснюватись легко, дистанційно та за допомогою електронних засобів, шляхом використання належного єдиного інформаційно-розрахункового центру відповідними органами. Крім того багато он-лайн послуг, доступних через єдиний інформаційно-розрахунковий центр потребують електронної ідентифікації, автентифікації та електронного підпису.
- (9) У більшості випадків громадяни не можуть використати свою електронну ідентифікацію для автентифікації в іншій державі-члені, оскільки національні схеми електронної ідентифікації в їх країні не визнаються на території інших держав-членів. Така цифрова перешкода заважає провайдерам послуг скористатися всіма перевагами внутрішнього ринку. Взаємне визнання засобів електронної ідентифікації полегшить транскордонне надання численних послуг на внутрішньому ринку і дозволить підприємствам вести транскордонну діяльність не стикаючись з численними перешкодами під час взаємодії з органами державної влади.
- (10) Директива 2011/24/ЄС Європейського Парламенту та Ради ⁽³⁾ запроваджує мережу національних органів влади, відповідальних за електронну систему охорони здоров'я. Для забезпечення безпеки і безперервності транскордонної системи охорони здоров'я, ця мережа повинна розробити керівні принципи, що стосуються транскордонного доступу до електронних даних про стан здоров'я і послуг, в тому числі шляхом підтримки «спільних заходів ідентифікації та автентифікації для полегшення передачі даних в рамках транскордонної системи охорони здоров'я». Взаємне визнання електронних ідентифікації та автентифікації є ключовим до того, щоб зробити транскордонну охорону здоров'я реальною для громадян Європи. Якщо громадяни подорожують з метою лікування, їх медичні дані повинні бути доступні в країні лікування. Останнє вимагає ґрунтовної, безпечної і надійної концепції в сфері електронної ідентифікації.
- (11) Цей Регламент повинен застосовуватися у повній відповідності з принципами, що стосуються захисту персональних даних, передбачених Директивою 95/46/ЄС Європейського Парламенту та Ради ⁽⁴⁾. З цього приводу, враховуючи запроваджений цим Регламентом принцип взаємного визнання, автентифікація для он-лайн послуги повинна стосуватися лише обробки тих ідентифікаційних даних, які є адекватними, належними та помірними для надання доступу до цієї он-лайн послуги. Крім того, провайдери довірчих послуг та контрольні органи повинні задовольняти передбаченим Директивою 95/46/ЄС вимогам щодо конфіденційності та безпеки обробки.
- (12) Однією з цілей цього Регламенту є усунення існуючих перешкод для транскордонного використання засобів електронної ідентифікації, що використовуються в державах-членах для автентифікації, щонайменше для систем надання громадських послуг. Цей Регламент не має на меті втручатися в системи управління електронною ідентифікацією і пов'язані з ними інфраструктури, засновані на території держав-членів. Цей Регламент має на меті переконатися в можливості проведення безпечної електронної ідентифікації та автентифікації, що стосується доступу до транскордонних он-лайн послуг, запропонованих державами-членами.

⁽¹⁾ ОВ С 50 від 21.2.2012, С. 1.

⁽²⁾ Директива 2006/123/ЄС Європейського Парламенту та Ради від 12 грудня 2006 року про послуги на внутрішньому ринку (ОВ L 376 від 27.12.2006, С. 36).

⁽³⁾ Директива 2011/24/ЄС Європейського Парламенту та Ради від 9 березня 2011 року про застосування прав пацієнтів в сфері транскордонного здійснення медичного обслуговування (ОВ L 88 від 4.4.2011, С. 45).

⁽⁴⁾ Директива 95/46/ЄС Європейського Парламенту та Ради від 24 жовтня 1995 року про захист фізичних осіб, що стосується обробки персональних даних та вільного обігу зазначених даних (ОВ L 281 від 23.11.1995, С. 31).

- (13) Держави-члени повинні залишати за собою право використовувати або вводити засоби для електронної ідентифікації і для доступу до он-лайн послуг. Вони також повинні вирішити, чи слід залучати приватний сектор до надання цих засобів. Держави-члени не зобов'язані нотифікувати Комісії їх схеми електронної ідентифікації. Вибір залишається за державою-членом: чи нотифікувати Комісії повною мірою або частково, або не нотифікувати жодну зі схем електронної ідентифікації, що використовуються на державному рівні для доступу щонайменше до громадських он-лайн послуг або спеціальних послуг.
- (14) В Регламенті повинні бути встановлені певні умови, що стосуються засобів електронної ідентифікації, які мають бути визнані, а також спосіб, у який повинні нотифікуватись схеми електронної ідентифікації. Такі умови повинні дозволити державам-членам створити необхідний рівень довіри в їх відповідних схемах електронної ідентифікації та полегшити взаємне визнання засобів електронної ідентифікації, що належать до їх нотифікованих схем. Принцип взаємного визнання повинен застосовуватись, якщо схема електронної ідентифікації держави-члена, що здійснює нотифікацію, відповідає умовам нотифікації та, якщо нотифікація була опублікована в *Офіційному віснику Європейського Союзу*. Проте, принцип взаємного визнання повинен стосуватись лише автентифікації для он-лайн послуг. Доступ до цих он-лайн послуг та їх кінцеве надання замовникові повинні бути тісно пов'язані з правом отримання таких послуг на умовах, встановлених національним законодавством.
- (15) Зобов'язання визнавати засоби електронної ідентифікації відноситься тільки до тих засобів, рівень гарантії яких відповідає або вище рівня, необхідного для обслуговування в он-лайн режимі. Крім того, зобов'язання має застосовуватись тільки коли відповідний орган державного сектора використовує «істотний» або «високий» рівень довіри по відношенню до он-лайн послуг. Відповідно до законодавства Європейського Союзу держави-члени повинні залишатись вільними у питанні визнання засобів електронної ідентифікації, що мають нижчий рівень достовірності ідентифікаційної інформації.
- (16) Рівні гарантії повинні характеризувати рівень достовірності засобу електронної ідентифікації під час встановлення ідентифікаційної інформації про особу, забезпечуючи тим самим гарантію того, що особа, яка потребує окремої ідентифікаційної інформації, є особою, якій було присвоєно зазначену ідентифікаційну інформацію. Рівень гарантії залежить від рівня достовірності, який надається засобом електронної ідентифікації для заявленої або стверджуваної ідентифікаційної інформації про будь-яку особу з урахуванням процесів (наприклад, підтвердження і перевірка ідентифікаційної інформації, автентифікація), діяльності з управління (наприклад, підрозділом, що надає засоби електронної ідентифікації, процедурами надання таких засобів), а також впровадженого технічного контролю. Різні технічні визначення та опис рівнів гарантії існують як результат заснованих в Європі великомасштабних пілотних проектів, стандартизації та міжнародної діяльності. Зокрема, великомасштабний пілотний проект STORK та стандарт ISO 29115 зазначають, між іншим, рівні 2, 3 і 4, які повинні ретельно враховуватись під час запровадження мінімальних технічних вимог, стандартів та процедур для рівнів гарантії «низький», «суттєвий» та «високий» відповідно до положень цього Регламенту, гарантуючи узгоджене застосування цього Регламенту, зокрема, що стосується найвищого рівня гарантії для підтвердження ідентифікаційної інформації під час видачі кваліфікованих сертифікатів. Встановлені вимоги повинні бути технологічно нейтральними. Повинно також бути забезпечено можливість для досягнення необхідних вимог безпеки шляхом використання різноманітних технологій.
- (17) Держави-члени повинні заохочувати приватний сектор добровільно використовувати засоби електронної ідентифікації, що належать до нотифікованої схеми, з метою ідентифікації, що вимагається он-лайн послугами або електронними транзакціями. Можливість використання таких засобів електронної ідентифікації дозволить приватному сектору покладатися на електронну ідентифікацію та автентифікацію, що вже широко використовується в багатьох державах-членах, принаймні в державних службах для полегшення підприємствам та громадянам доступу до їхніх транскордонних он-лайн послуг. З метою полегшення транскордонного використання приватним сектором таких засобів електронної ідентифікації передбачена будь-якою державою-членом можливість автентифікації повинна бути доступною для сторін-користувачів приватного сектора, заснованих поза межами території держави-члена на таких самих умовах, як ті, що застосовуються для сторін-користувачів приватного сектора в межах держави-члена. Отже, що стосується сторін-користувачів приватного сектору держава-член, що здійснює нотифікацію, може визначити умови доступу до засобів автентифікації. Такими умовами доступу може зазначатись чи є на даний час доступним для сторін-користувачів приватного сектора засіб автентифікації, що відноситься до нотифікованої схеми.
- (18) Цей Регламент передбачає відповідальність держави-члена, що здійснює нотифікацію, сторони, що випускає засоби електронної ідентифікації та сторони, що проводить процедури автентифікації, за невиконання відповідних зобов'язань, визначених цим Регламентом. Проте, зазначений Регламент повинен застосовуватись відповідно до національних норм в сфері відповідальності. Таким чином, він не впливає на ці норми, наприклад, з питань щодо визначення збитків або на прийняті процесуальні

норми, у тому числі норми, що стосуються тягаря доказування.

- (19) Безпека схем електронної ідентифікації є ключем для забезпечення надійності транскордонного взаємного визнання засобів електронної ідентифікації. У цьому контексті держави-члени повинні співпрацювати відносно безпеки та сумісності схем електронної ідентифікації на рівні Європейського Союзу. Кожного разу, коли схеми електронної ідентифікації вимагають специфічного обладнання або програмного забезпечення, яке буде використовуватися сторонами-користувачами на національному рівні, транскордонна сумісність вимагає того, щоб держави-члени не нав'язували такі вимоги і пов'язані з ними витрати для сторін-користувачів, заснованих поза межами їх (держав-членів) територій. У цьому випадку відповідні рішення повинні бути обговорені і розроблені в рамках інфраструктури сумісності. Проте, вплив технічних вимог, що випливають із національних специфікацій засобів електронної ідентифікації, на держателів таких електронних засобів (наприклад, смарт-карт) є неминучим.
- (20) Співробітництво держав-членів повинно сприяти встановленню технічної сумісності схем електронної ідентифікації, нотифікованих з метою створення високого рівня довіри і безпеки, що відповідає ступеню ризику. Обмін інформацією та спільне користування передовим досвідом між державами-членами з метою їх взаємного визнання повинно полегшити таке співробітництво.
- (21) Цей Регламент повинен також запровадити загальні правові рамки, що стосуються використання електронних довірчих послуг. Проте, це не повинно створювати загального зобов'язання використовувати їх або встановлювати точку доступу для всіх існуючих електронних довірчих послуг. Зокрема, дія загальних правових рамок не повинна розповсюджуватись на надання послуг, що використовуються між певною групою учасників виключно в закритих системах, які не мають жодного впливу на третіх осіб. Наприклад системи, що створені в корпорації або державних адміністраціях для управління внутрішніми процедурами з використанням довірчих послуг не повинні враховувати вимоги цього Регламенту. Тільки довірчі послуги, що надаються державними організаціями, мають вплив на третіх осіб і повинні відповідати вимогам, викладеним у Регламенті. Не слід застосовувати вимоги Регламенту щодо аспектів, пов'язаних з укладенням та дією договорів або інших юридичних зобов'язань, де є вимоги до форми і в загальному випадку визначаються національним або союзним законом. Не слід також чіпати національні вимоги щодо форм, які стосуються державних реєстрів, зокрема комерційних і земельних.
- (22) Для того, щоб внести електронні довірчі послуги у загальну систему транскордонного використання, повинна існувати можливість використовувати їх як докази в ході судового розгляду в усіх державах-членах. Саме національне законодавство повинне визначити юридичну силу довірчих послуг, якщо інше не передбачено цим Регламентом.
- (23) Тією ж мірою, що цей Регламент визначає зобов'язання відносно визнання довірчих послуг, відповідна довірча послуга може бути відхилена тільки в тому випадку, коли адресат не зможе прочитати або перевірити її сутність з технічних причин, які перебувають поза безпосереднім контролем адресату. Проте, це зобов'язання про визнання не повинно саме по собі вимагати від державного органу придбання апаратного та програмного забезпечень, які необхідні для технічної обробки усіх існуючих довірчих послуг.
- (24) Держави-члени можуть застосовувати діючі або вводити національні положення, що відповідають законодавству Європейського Союзу, які стосуються довірчих послуг, якщо ці послуги не повною мірою узгоджені з цим Регламентом. Проте, довірчі послуги, які відповідають цьому Регламенту, повинні вільно застосовуватись на внутрішньому ринку.
- (25) Держави-члени додатково до тих довірчих послуг, що входять в закритий перелік, передбачений цим Регламентом, повинні бути вільними у визначенні інших довірчих послуг з метою їх визнання на національному рівні як кваліфікованих довірчих послуг.
- (26) Враховуючи швидкий темп технологічного розвитку цей Регламент повинен закріпити відкритий для інновацій підхід.
- (27) Цей Регламент повинен бути технологічно нейтральним. Його правові наслідки повинні бути досяжні за допомогою наявних будь-яких технічних засобів, що задовольняють вимогам цього Регламенту.

- (28) З метою підвищення довіри малих та середніх підприємств та населення на внутрішньому ринку та сприяння використанню довірчих продуктів і послуг, визначення кваліфікованих довірчих послуг та провайдерів кваліфікованих довірчих послуг повинні вводитись з метою висвітлення вимог та зобов'язань щодо забезпечення високого рівня безпеки всіх кваліфікованих довірчих послуг і продуктів, що використовуються або надаються
- (29) Відповідно до зобов'язань по Конвенції Організації Об'єднаних Націй про права інвалідів, схваленої Рішенням Ради 2010/48/ЄС ⁽¹⁾, зокрема її статті 9, інваліди повинні мати можливість використовувати довірчі послуги, а також продукти, призначені для кінцевих споживачів, що слугують для надання таких послуг, на тих самих умовах, що і інші споживачі. Надані довірчі послуги, а також продукти, призначені для кінцевих користувачів, які слугують для надання зазначених послуг повинні таким чином бути в міру можливого доступними для інвалідів. Оцінка доцільності повинна враховувати, між іншим, технічні та економічні міркування.
- (30) На підставі цього Регламенту держави-члени призначають наглядовий орган або наглядові органи, уповноважені на здійснення наглядової діяльності. Держави-члени повинні також мати можливість вирішувати, за взаємною згодою з іншою державою-членом, питання призначення контрольного органу на території цієї іншої держави-члена.
- (31) Наглядові органи повинні співпрацювати з органами з нагляду за дотриманням законодавства про захист персональних даних, наприклад інформуючи останніх про результати перевірок провайдерів кваліфікованих довірчих послуг, якщо виявляється, що були порушені норми в сфері захисту персональних даних. Надання інформації повинно включати зокрема повідомлення про інциденти безпеки та порушення щодо захисту персональних даних.
- (32) З метою підвищення рівня довіри користувачів на єдиному ринку на всіх провайдерів довірчих послуг повинно бути накладено зобов'язання застосовувати належні практики безпеки, що відповідали б ризикам, пов'язаним з їх діяльністю.
- (33) Положення про використання псевдонімів у сертифікатах не повинні перешкоджати державам-членам вимагати здійснення ідентифікації осіб відповідно до національного законодавства або законодавства Європейського Союзу.
- (34) Усі держави-члени повинні задовольняти основним спільним вимогам з нагляду з метою забезпечення порівняного рівня безпеки в сфері кваліфікованих довірчих послуг. Для полегшення узгодженого застосування цих вимог на території Європейського Союзу, держави-члени повинні ухвалити відповідні процедури та здійснювати обмін інформацією про їх наглядову діяльність та передовий досвід в цій сфері.
- (35) Усі провайдери довірчих послуг повинні підлягати вимогам цього Регламенту, зокрема з питань безпеки та відповідальності, для забезпечення належної обачності, прозорості та підзвітності стосовно їх діяльності та послуг. Проте, враховуючи тип послуг, що надаються провайдерами довірчих послуг, доцільно розрізняти, наскільки ці вимоги стосуються провайдерів кваліфікованих та некваліфікованих довірчих послуг.
- (36) Запровадження наглядового режиму для всіх провайдерів довірчих послуг повинне забезпечити справедливі умови конкуренції, що стосується безпеки та відповідальності по відношенню до їх діяльності та їх послуг і сприяти, таким чином, захисту споживачів та функціонуванню внутрішнього ринку. Некваліфіковані провайдери довірчих послуг повинні бути суб'єктами спрощеної та постфактум наглядової діяльності, що відповідає характеру їх послуг та здійснюваних ними операцій. У зв'язку з цим, наглядовий орган не повинен мати загального зобов'язання щодо нагляду за некваліфікованими провайдерами послуг. Наглядовий орган повинен вживати заходи тільки у разі його повідомлення (наприклад, самим некваліфікованим провайдером довірчих послуг, іншим наглядовим органом, користувачем або діловим партнером, або на підставі власного розслідування) про те, що некваліфікований провайдер довірчих послуг не виконує вимоги Регламенту.

⁽¹⁾ Рішення Ради 2010/48/ЄС від 26 листопада 2009 року щодо укладення Європейським Співтовариством Конвенції ООН про права інвалідів (ОВ L 23 від 27.1.2010, С. 35).

- (37) Цей Регламент передбачає відповідальність всіх провайдерів довірчих послуг. Зокрема, ним запроваджується режим відповідальності, відповідно до якого всі провайдери довірчих послуг повинні нести відповідальність за шкоду, завдану будь-якій фізичній або юридичній особі в результаті недотримання зобов'язань, передбачених цим Регламентом. З метою полегшення оцінки фінансового ризику, який, можливо, провайдерам довірчих послуг доведеться нести та покривати за рахунок страхових полісів, цей Регламент дозволяє останнім встановлювати, за певних умов, обмеження у використанні запропонованих ними послуг та не нести відповідальність за шкоду, завдану внаслідок перевищеного використання зазначених послуг. Клієнти повинні бути належним чином заздалегідь поінформованими про встановлені обмеження. Ці обмеження повинні бути узгоджені з третьою стороною, наприклад, шляхом включення інформації про це в умови надання послуги або шляхом використання інших узгоджених засобів. Для цілей введення в дію цих принципів, цей Регламент повинен застосовуватися відповідно до національних норм в сфері відповідальності. Отже, цей Регламент не впливає на зазначені національні норми, наприклад, норми, що стосуються визначення збитків, завданих навмисно або внаслідок недбалості або процесуальні норми, що застосовуються в цій сфері.
- (38) Повідомлення про порушення безпеки та оцінка ризиків безпеки є необхідними для надання адекватної інформації зацікавленим сторонам у разі порушення безпеки або втрати цілісності.
- (39) Для надання можливості Комісії та державам-членам оцінити ефективність механізму повідомлення про порушення, який вводиться цим Регламентом, наглядові органи повинні здійснювати надання за запитом підсумкової інформації для Комісії та Європейського агентства з мережевої та інформаційної безпеки.
- (40) Для надання можливості Комісії та державам-членам оцінити ефективність удосконаленого механізму нагляду, який вводиться цим Регламентом, наглядовим органам повинно бути доручено звітувати про свою діяльність. Це відіграло б важливу роль у спрощенні обміну передовим досвідом між наглядовими органами та забезпечило б перевірку повноти та ефективності реалізації основних вимог щодо нагляду у всіх державах-членах.
- (41) З метою забезпечення безперервності та довговічності кваліфікованих довірчих послуг, а також для підвищення рівня довіри, що стосується впевненості користувачів у безперервності надання кваліфікованих довірчих послуг, наглядові органи повинні перевірити наявність і належне застосування положень планів припинення діяльності на випадок припинення діяльності провайдерами кваліфікованих довірчих послуг.
- (42) Для сприяння нагляду за провайдерами кваліфікованих довірчих послуг, наприклад, коли провайдер надає свої послуги на території іншої держави-члена і не підлягає там нагляду, або коли комп'ютери провайдера знаходяться на території іншої держави-члена, ніж та, до якої належить провайдер, повинна бути створена взаємна система допомоги між наглядовими органами в державах-членах.
- (43) З метою забезпечення відповідності провайдерів кваліфікованих довірчих послуг та послуг, які вони надають, вимогам, викладених у цьому Регламенті, повинна здійснюватися оцінка відповідності органом з оцінки відповідності, а отримані звіти з оцінки відповідності повинні бути представлені провайдерами кваліфікованих довірчих послуг до наглядового органу. Кожного разу, коли наглядовий орган вимагає від провайдера кваліфікованих довірчих послуг звіт з оцінки відповідності, наглядовий орган повинен дотримуватись зокрема принципу коректного управління, враховуючи зобов'язання щодо обґрунтованості своїх рішень, а також принципу пропорційності. Таким чином, наглядовий орган повинен належним чином мотивувати рішення щодо наданих матеріалів з оцінки відповідності.
- (44) Цей Регламент спрямований на створення узгодженої системи з метою забезпечення високого рівня безпеки та правової визначеності електронних довірчих послуг. У зв'язку з цим, при розгляді оцінки відповідності продукції та послуг, Комісія, за необхідності, повинна взаємодіяти з відповідними існуючими європейськими та міжнародними схемами, такими як Регламент (ЄС) № 765/2008 Європейського Парламенту та Ради ⁽¹⁾ щодо визначення вимог до акредитації та нагляду за ринком.

⁽¹⁾ Регламент № 765/2008 Європейського Парламенту та Ради від 9 липня 2008 року, яким встановлюються приписи щодо акредитації та нагляду за ринком в процесі розміщення товарів на ринку і яким скасовується Регламент Ради (ЄЕС) №. 339/83 (ОВ L 218 від 13.8.2008, С. 30).

- (45) З метою забезпечення ефективного процесу запуску, який призвів би до включення провайдерів кваліфікованих довірчих послуг і кваліфікованих довірчих послуг, які вони надають, в довірчі списки, належить заохочувати до попередньої взаємодії потенційного провайдера кваліфікованих довірчих послуг і компетентного наглядового органу з метою сприяння забезпеченню належної сумлінності під час підготовки до надання кваліфікованих довірчих послуг.
- (46) Довірчі списки є важливими елементами для зміцнення довіри між учасниками ринку, оскільки вони є показником кваліфікованого статусу провайдера довірчих послуг під час здійснення нагляду.
- (47) Зручність он-лайн послуг і впевненість в них є основними для того, щоб користувачі могли повною мірою скористатися і свідомо розраховувати на електронні послуги. З цієї метою створюється знак довіри ЄС для ідентифікації кваліфікованих довірчих послуг, що надаються кваліфікованими провайдерами довірчих послуг. Такий знак довіри ЄС до кваліфікованих довірчих послуг дозволить чітко відрізнити кваліфіковані довірчі послуги від інших довірчих послуг, сприяючи підвищенню прозорості ринку. Використання знаку довіри ЄС провайдерами кваліфікованих довірчих послуг має бути добровільним і не повинно ґрунтуватись на інших вимогах, ніж ті, що вже передбачені цим Регламентом.
- (48) У той час як для забезпечення взаємного визнання електронних підписів необхідним є високий рівень безпеки, в певних випадках, наприклад, в контексті Рішення Комісії 2009/767/ЄС ⁽¹⁾, також повинні прийматися електронні підписи з нижчим рівнем забезпечення безпеки.
- (49) Цей Регламент встановлює принцип, що електронний підпис не повинен позбавлятися юридичної сили на тій підставі, що він представлений в електронному вигляді, або, що він не відповідає вимогам кваліфікованого електронного підпису. Проте, національному законодавству належить визначати юридичну силу електронних підписів, за винятком вимог, передбачених у цьому Регламенті, відповідно до яких кваліфікований електронний підпис повинен мати юридичну силу еквівалентну власноручному підпису.
- (50) Оскільки компетентні органи на території держав-членів на даний час використовують різні формати удосконалених електронних підписів для проставлення їх на документи в електронному вигляді, необхідно щоб принаймні декілька форматів удосконалених електронних підписів мали технічну підтримку в державах-членах, які отримують документи, підписані в електронному вигляді. Подібним чином, коли компетентні органи в державах-членах використовують удосконалені електронні печатки, було б необхідно забезпечити, щоб вони підтримували принаймні декілька форматів удосконалених електронних печаток.
- (51) Підписувач повинен мати можливість доручити кваліфіковані засоби створення електронного підпису третім особам, за умови, що будуть запроваджені належні механізми та процедури, що гарантують одноосібний контроль підписувача за його даними створення електронного підпису, а також за умови, що використання зазначених засобів відповідає вимогам в сфері кваліфікованого електронного підпису.
- (52) Можливість створення віддалених електронних підписів від імені підписувача в умовах управління провайдером довірчих послуг середовищем створення електронних підписів надається у світлі підвищення численних економічних вигод. Проте для того, щоб гарантувати, що такі електронні підписи отримують рівне юридичне визнання як і електронні підписи, що створені в середовищі, повністю керованому користувачем, провайдери послуг віддаленого підпису повинні застосовувати спеціальні управлінські та адміністративні процедури безпеки, а також використовувати надійні системи і продукти, у тому числі безпечні канали електронного зв'язку, з метою забезпечення надійності середовища створення електронних підписів та одноосібного контролю за середовищем з боку користувача. Якщо кваліфікований електронний підпис створюється за допомогою засобу створення віддаленого електронного підпису, то повинні застосовуватися вимоги до кваліфікованих провайдерів довірчих послуг, наведені у цьому Регламенті.

⁽¹⁾ Рішення Комісії 2009/767/ЄС від 16 жовтня 2009 про запровадження заходів, призначених для полегшення виконання процедур в електронному режимі шляхом використання єдиного інформаційно-розрахункового центру відповідно до Директиви 2006/123/ЄС Європейського Парламенту та Ради про послуги на внутрішньому ринку (ОВ L 274 від 20.10.2009, С. 36).

- (53) Тимчасове призупинення дії кваліфікованих сертифікатів є в певній кількості держав-членів діючою практикою, запровадженою провайдерами довірчих послуг, яка відрізняється від відкликання і призводить до тимчасової втрати дійсності сертифіката. Правова визначеність вимагає того, щоб статус тимчасового призупинення дії сертифікату був завжди чітко зазначеним. З цією метою на провайдерів довірчих послуг повинна покладатись відповідальність чітко зазначати статус сертифікату та, якщо дія останнього призупинена, вказувати точний період часу, протягом якого дія сертифікату буде призупинена. Цей Регламент не повинен зобов'язувати провайдерів довірчих послуг або держави-члени використовувати тимчасове призупинення дії, але повинен передбачати норми в сфері прозорості у випадку доступності такої практики.
- (54) Транскордонна сумісність і визнання кваліфікованих сертифікатів є попередньою умовою для транскордонного визнання кваліфікованих електронних підписів. Отже до кваліфікованих сертифікатів не повинно висуватись жодних обов'язкових вимог, що перевищують вимоги, викладені в цьому Регламенті. Проте, на національному рівні має бути дозволено включення до кваліфікованих сертифікатів спеціальних характеристик, таких як унікальні ідентифікатори, але за умови, що такі спеціальні характеристики не перешкоджають транскордонній сумісності та визнанню кваліфікованих сертифікатів та електронних підписів.
- (55) Сертифікація ІТ - безпеки на основі міжнародних стандартів, наприклад, ISO 15408 та пов'язані з цим методи оцінки та угоди про взаємне визнання є важливим інструментом для перевірки безпеки засобів створення кваліфікованого підпису, застосування якого повинно заохочуватися. Проте, інноваційні рішення і послуги, такі як підписання в мобільних системах та підписання в інформаційній системі «хмари», потребують технічного та організаційного рішення для тих кваліфікованих засобів створення електронного підпису, для яких поки що може не бути стандартів безпеки або для яких безпосередньо в цей час проводиться перевірка першої сертифікації засобів захисту. Рівень безпеки зазначених кваліфікованих засобів може бути оцінений шляхом використання інших процесів лише, якщо зазначені стандарти безпеки не існують або, якщо безпосередньо в цей час проводиться перевірка першої сертифікації інформаційної безпеки. Ці процеси повинні бути порівняними зі стандартами сертифікації ІТ – безпеки тією мірою, наскільки їх рівні безпеки є еквівалентними. Ці процеси могли б бути полегшені завдяки використанню партнерської перевірки.
- (56) Цим Регламентом повинні запроваджуватись вимоги, що застосовуються до кваліфікованих засобів для створення підпису для забезпечення функціональності удосконалених електронних підписів. Цей Регламент не повинен охоплювати все системне середовище, в якому функціонують такі пристрої. Таким чином, сфера сертифікації кваліфікованих засобів створення електронного підпису не повинна виходити за межі апаратного та системного програмного забезпечення, які використовуються для управління та захисту даних для створення електронних підписів, які створюються, зберігаються або оброблюються засобами створення електронного підпису. Як докладно зазначено у відповідних стандартах, прикладні програми створення електронного підпису не повинні підлягати обов'язковій сертифікації.
- (57) Для забезпечення правової визначеності, що стосується чинності підпису необхідно визначити, які компоненти кваліфікованого електронного підпису мають бути перевірені стороною, що здійснює перевірку підпису. Крім того, визначення вимог до провайдерів кваліфікованих довірчих послуг, які можуть надавати кваліфіковану послугу перевірки відповідним сторонам, що не бажають або не в змозі самостійно проводити перевірки кваліфікованого електронного підпису, має стимулювати приватний та державний сектор до інвестування в такі послуги. Обидві складові повинні зробити перевірку кваліфікованого електронного підпису простою і зручною для всіх сторін на рівні Європейського Союзу.
- (58) У випадках, коли транзакція передбачає використання юридичною особою кваліфікованої електронної печатки, також рівнозначно повинен прийматися кваліфікований електронний підпис уповноваженого представника юридичної особи.
- (59) Електронні печатки повинні служити доказом того, що електронний документ був виданий юридичною особою, забезпечуючи достовірність походження документа та його цілісність.
- (60) Провайдери довірчих послуг, які видають кваліфіковані сертифікати для електронної печатки, повинні запровадити необхідні заходи для того, щоб мати можливість встановити відомості про особу для фізичної особи, яка представляє юридичну особу, якій надається кваліфікований сертифікат для електронної печатки, у разі, коли така ідентифікація є необхідною на національному рівні в рамках судових чи адміністративних проваджень.

- (61) Цей Регламент повинен забезпечити довгострокове збереження інформації з метою забезпечення юридичної сили електронного підпису та електронних печаток протягом тривалого періоду часу, а також гарантувати, що останні зможуть бути чинними незалежно від технічного прогресу.
- (62) З метою забезпечення безпеки кваліфікованих позначок часу, Регламент повинен зобов'язати використовувати удосконалену електронну печатку, удосконалений електронний підпис або інші еквівалентні методи. Можна передбачати, що нововведення може привести до появи нових технологій, які можуть забезпечити еквівалентний рівень безпеки для позначок часу. В разі використання іншого методу, ніж удосконалена електронна печатка або удосконалений електронний підпис, провайдером кваліфікованих довірчих послуг повинно бути доведено в звіті про оцінку відповідності, що зазначений метод забезпечує еквівалентний рівень безпеки та задовольняє всім зобов'язанням, передбаченим цим Регламентом.
- (63) Електронні документи мають важливе значення для подальшого розвитку транскордонних електронних транзакцій на внутрішньому ринку. Цим Регламентом повинно бути запроваджено принцип, відповідно до якого електронний документ не повинен бути позбавлений юридичної сили на тій підставі, що він має електронну форму, для забезпечення того, що електронна транзакція не буде відхилена лише на тій підставі, що документ має електронну форму.
- (64) При вирішенні питання форматів удосконалених електронних підписів і печаток, Комісія повинна спиратися на чинні практики, стандарти та законодавчі положення, зокрема рішення Комісії 2011/130/ЄС ⁽¹⁾.
- (65) Окрім перевірки достовірності документа, виданого юридичною особою, електронні печатки можуть бути використані для автентифікації будь-яких цифрових активів юридичної особи, наприклад, програмного коду, серверів.
- (66) Необхідно передбачити правові рамки з метою полегшення транскордонного визнання між існуючими національними правовими системами в сфері послуг рекомендованих електронних відправлень. Такі рамки могли б також відкрити нові ринкові можливості, що дозволяють провайдерам довірчих послуг Європейського Союзу запропонувати нові загальноєвропейські послуги рекомендованих електронних відправлень.
- (67) Послуги автентифікації веб-сайту надають засоби, за допомогою яких відвідувач веб-сайту може бути впевнений, що за веб-сайтом стоїть реальна і легітимна організація. Такі послуги сприяють зміцненню довіри і впевненості по відношенню до веб-сайту, з огляду на те, що користувачі будуть мати впевненість у справжності веб-сайту, оскільки він перевіряється на автентичність. Надання і використання послуги автентифікації веб-сайту є повністю добровільними. Проте для того, щоб перевірка справжності веб-сайту стала засобом підвищення довіри та забезпечувала впровадження найкращого досвіду в інтересах користувача і подальшого зростання його використання на внутрішньому ринку, цей Регламент встановлює мінімальні рівні безпеки та зобов'язань для провайдерів та для їх послуг. З цією метою було враховано результати існуючих галузевих ініціатив (наприклад, Certification Authorities/Browsers Forum - CA/B Forum). Крім того, цей Регламент не повинен заважати використанню інших засобів або методів автентифікації веб-сайту, на які не розповсюджується дія цього Регламенту, а також не повинні перешкоджати провайдерам послуг автентифікації веб-сайту третіх країн надавати послуги для клієнтів на території Європейського Союзу. Проте, послуги автентифікації веб-сайту, що надаються провайдером з третьої країни, визнаються кваліфікованими на підставі цього Регламенту лише якщо між Європейським Союзом та країною заснування зазначеного провайдера було укладено міжнародну угоду.
- (68) Поняття «юридична особа», відповідно до положень Договору про функціонування Європейського Союзу, що стосуються заснування, залишає за учасниками ринку вибір юридичної форми, яку вони вважали б за належну для здійснення їх діяльності. Отже, "юридична особа", відповідно до змісту Договору про функціонування Європейського Союзу, означає будь-яку організацію, що була заснована на підставі права держави-члена або діяльність якої регулюється правом держави-члена, незалежно від її правової форми.
- (69) Установи органи та організації Європейського Союзу заохочуються до визнання електронної ідентифікації та довірчих послуг, на які розповсюджується дія цього Регламенту, з метою адміністративного співробітництва з отриманням вигоди, зокрема від існуючих належних практик та результатів поточних проектів в сферах, на які розповсюджується дія цього Регламенту.

⁽¹⁾ Рішення Комісії 2011/130/ЄС від 25 лютого 2011 року про запровадження мінімальних вимог для транскордонної обробки документів з електронними підписами, проставленими компетентними органами відповідно до Директиви 2006/123/ЄС Європейського Парламенту та Ради про послуги на внутрішньому ринку (ОВ L 53 від 26.2.2011, С. 66).

- (70) З метою гнучкого та швидкого доповнення певних детальних технічних аспектів цього Регламенту, належить делегувати Комісії повноваження приймати акти відповідно до статті 290 Договору про функціонування Європейського Союзу, що стосується критеріїв, яким повинні відповідати органи сертифікації засобів створення кваліфікованого електронного підпису. Зокрема важливо, щоб Комісія проводила належні консультації в ході своєї підготовчої роботи, в тому числі на рівні експертів. Комісія при підготовці і складанні делегованих актів, повинна забезпечити одночасну, своєчасну та належну передачу відповідних документів до Європейського Парламенту та Ради.
- (71) З метою забезпечення єдиних умов для виконання цього Регламенту, повноваження щодо реалізації повинні бути покладені на Комісію, зокрема, що стосується зазначення реєстраційних номерів стандартів, використання яких надасть презумпцію відповідності певним вимогам, викладеним у цьому Регламенті. Ці повноваження повинні здійснюватися відповідно до Регламенту (ЄС) №182/2011 Європейського Парламенту та Ради ⁽¹⁾.
- (72) При прийнятті делегованих або виконавчих актів, з метою забезпечення високого рівня безпеки та сумісності для електронної ідентифікації та довірчих послуг, Комісія повинна належним чином враховувати стандарти та технічні специфікації, які розроблено європейськими і міжнародними організаціями та органами стандартизації, зокрема Європейським комітетом з стандартизації, Європейським інститутом стандартизації електрозв'язку, Міжнародною організацією з стандартизації та Міжнародним союзом електрозв'язку.
- (73) З метою правової визначеності та ясності, Директива 1999/93/ЄС повинна бути скасована.
- (74) Для забезпечення правової визначеності для учасників ринку, що вже використовують кваліфіковані сертифікати електронного підпису, видані фізичним особам відповідно до Директиви 1999/93/ЄС, належить передбачити достатній строк для перехідного періоду. Так само, перехідні заходи повинні бути передбачені для засобів створення безпечних підписів, відповідність яких була визначена на підставі Директиви 1999/93/ЄС, а також для провайдерів послуг сертифікації, що видадуть кваліфіковані сертифікати до 1 липня 2016 року. Нарешті, також необхідно забезпечити Комісію засобами для прийняття виконавчих та делегованих актів.
- (75) Строки застосування, що викладені в цьому Регламенті, не впливають на існуючі зобов'язання, які держави-члени вже взяли на себе відповідно до законодавства Європейського Союзу, зокрема відповідно до Директиви 2006/123/ЄС.
- (76) Оскільки цілі цього Регламенту не можуть бути достатньою мірою досягнуті окремими державами-членами, але можуть, враховуючи масштаби заходів, бути кращою мірою досягнутими на рівні Європейського Союзу, останній може вжити заходи відповідно до принципу субсидіарності, зазначеного в статті 5 Договору про Європейський Союз. Відповідно до принципу пропорційності, викладеного у вказаній статті, цей Регламент не виходить за рамки необхідного для досягнення зазначеної мети,
- (77) Відповідно до частини 2 статті 28 Регламенту (ЄС) № 45/2001 Європейського Парламенту та Ради ⁽²⁾ були проведені консультації з Європейським наглядовим органом із захисту даних та останнім було надано висновок 27 вересня 2012 року ⁽³⁾,

⁽¹⁾ Регламент (ЄС) № 182/2011 Європейського Парламенту та Ради від 16 лютого 2011 року про запровадження загальних норм та принципів щодо порядку контролю державами-членами реалізації Комісією виконавчих повноважень (ОВ L 55 від 28.2.2011, С. 13).

⁽²⁾ Регламент (ЄС) № 45/2001 Європейського Парламенту та Ради від 18 грудня 2000 року про захист фізичних осіб від обробки персональних даних інституціями та органами Співтовариства та про вільний обіг даних (ОВ L 8 від 12.1.2001, С. 1)

⁽³⁾ ОВ С 28 від 30.1.2013, С. 6.

УХВАЛИЛИ ЦЕЙ РЕГЛАМЕНТ

РОЗДІЛ I

ЗАГАЛЬНІ ПОЛОЖЕННЯ

*Стаття 1***Предмет**

Для забезпечення належного функціонування внутрішнього ринку маючи на меті забезпечити адекватний рівень безпеки засобів електронної ідентифікації та довірчих послуг, цей Регламент:

- (a) встановлює умови, згідно з якими будь-яка держава-член визнає засоби електронної ідентифікації фізичних та юридичних осіб, що належать до схеми електронної ідентифікації, нотифікованої іншою державою-членом;
- (b) запроваджує норми, що застосовуються до довірчих послуг, зокрема для електронних транзакцій; та
- (c) встановлює правову основу для електронних підписів, електронних печаток, електронних позначок часу, електронних документів, послуг рекомендованих електронних відправлень та обслуговування сертифікатів для послуг автентифікації веб-сайтів.

*Стаття 2***Сфера застосування**

1. Цей Регламент застосовуються до схем електронної ідентифікації, які були нотифіковані державою-членом, а також до провайдерів довірчих послуг, заснованих на території Європейського Союзу.
2. Цей Регламент не поширюється на надання довірчих послуг, що використовуються виключно в закритих системах, які спираються на національні законодавства або угоди між певним переліком учасників.
3. Цей Регламент не впливає на національне законодавство або законодавство Європейського Союзу, пов'язане з укладанням та строком дії договорів або інших законних чи процесуальних зобов'язань, що стосується форми.

*Стаття 3***Визначення**

В цілях цього Регламенту застосовуються такі визначення:

- (1) "електронна ідентифікація" - процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну або юридичну особу або фізичну особу, що представляє юридичну особу;
- (2) "засоби електронної ідентифікації"- матеріальна та/або нематеріальна складова, яка містить дані персональної ідентифікації і використовується для автентифікації в он-лайн послугах;
- (3) "дані персональної ідентифікації" – сукупність даних, яка дозволяє встановити відомості про особу для фізичних або юридичних осіб або для фізичної особи, що представляє юридичну особу;
- (4) "схема електронної ідентифікації" - система електронної ідентифікації, на підставі якої засоби електронної ідентифікації видаються фізичним або юридичним особам або фізичним особам, що представляють юридичних осіб;

- (5) "автентифікація" - електронний процес, що дозволяє підтвердити електронну ідентифікацію фізичної або юридичної особи; або походження та цілісність даних в електронній формі;
- (6) "сторона-користувач" - фізична або юридична особа, яка покладається на електронну ідентифікацію або довірчу послугу;
- (7) "орган державного сектору" – Держава, регіональні або місцеві органи влади, установи публічного права та об'єднання, утворені одним або декількома органами влади, однією або декількома установами публічного права або приватні особи, уповноважені, принаймні одним або однією з таких органів влади, установ або об'єднань, надавати державні послуги, якщо останні діють на підставі цих повноважень;
- (8) "установа публічного права" – установа відповідно до визначення в пункті 4 частини 1 статті 2 Директиви 2014/24/ЄС Європейського Парламенту та Ради ⁽¹⁾
- (9) "підписувач" - це фізична особа, яка створює електронний підпис;
- (10) "електронний підпис" - дані в електронній формі, які приєднуються або логічно пов'язуються з іншими електронними даними, і використовуються підписувачем в якості підпису;
- (11) "удосконалений електронний підпис" - електронний підпис, який відповідає вимогам, викладеним у статті 26;
- (12) "кваліфікований електронний підпис" - удосконалений електронний підпис, який створюється засобом для створення кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті для електронних підписів;
- (13) "дані для створення електронного підпису" - унікальні дані, які використовуються підписувачем для створення електронного підпису;
- (14) "сертифікат електронного підпису" – електронне свідоцтво, що пов'язує дані для перевірки електронного підпису з фізичною особою та підтверджує принаймні ім'я або псевдонім цієї особи;
- (15) "кваліфікований сертифікат електронного підпису" – сертифікат електронного підпису, який видається кваліфікованим провайдером довірчих послуг і відповідає вимогам, закріпленим у Додатку I;
- (16) "довірча послуга" - електронна послуга, що зазвичай надається за винагороду і яка полягає у:
 - (a) створенні, перевірці та підтвердженні електронних підписів, електронних печаток або електронних позначок часу, послугах рекомендованих електронних відправлень та використанні сертифікатів, що пов'язані з цими послугами; або
 - (b) створенні, перевірці та підтвердженні сертифікатів для автентифікації веб-сайту; або
 - (c) збереженні електронних підписів, електронних печаток або сертифікатів, пов'язаних з цими послугами;
- (17) "кваліфікована довірча послуга" - це довірча послуга, яка відповідає вимогам цього Регламенту;

⁽¹⁾ Директива 2014/24/ЄС Європейського Парламенту та Ради від 26 лютого 2014 року про державні закупівлі та про скасування Директиви 2004/18/ЄС (ОВ L 94 від 28.3.2014, С. 65).

- (18) "орган оцінки відповідності" - орган, визначений у пункті 13 статті 2 Регламенту (ЄС) № 765/2008, акредитований відповідно до зазначеного Регламенту як компетентний у здійсненні оцінки відповідності кваліфікованого провайдера довірчих послуг та кваліфікованих довірчих послуг, які надаються зазначеним провайдером;
- (19) "провайдер довірчих послуг" - фізична або юридична особа, яка надає одну або декілька довірчих послуг. Існують кваліфіковані та некваліфіковані провайдери довірчих послуг;
- (20) "кваліфікований провайдер довірчих послуг" - провайдер довірчих послуг, який надає одну або декілька кваліфікованих довірчих послуг та має статус кваліфікованого, наданий йому наглядовим органом;
- (21) "продукт" – це апаратне або програмне забезпечення, або їх відповідні складові, які призначені для використання під час надання довірчих послуг;
- (22) "засіб для створення електронного підпису" - налаштоване програмне або апаратне забезпечення, яке використовується для створення електронного підпису;
- (23) "засіб для створення кваліфікованого електронного підпису" - засіб для створення електронного підпису, що відповідає вимогам, викладеним у Додатку II;
- (24) "розробник печатки" - юридична особа, яка створює електронну печатку;
- (25) "електронна печатка" - дані в електронній формі, які додаються або логічно пов'язані з іншими електронними даними для підтвердження походження та цілісності останніх;
- (26) "удосконалена електронна печатка" - електронна печатка, яка відповідає вимогам, зазначеним у статті 36;
- (27) "кваліфікована електронна печатка" - удосконалена електронна печатка, яка створюється засобом для створення кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки;
- (28) "дані для створення електронної печатки" - унікальні дані, які використовуються розробником електронної печатки для створення електронної печатки;
- (29) "сертифікат для електронної печатки" – електронне підтвердження, що пов'язує дані для перевірки електронної печатки з юридичною особою та підтверджує назву цієї особи;
- (30) "кваліфікований сертифікат для електронної печатки" - сертифікат для електронної печатки, який видається кваліфікованим провайдером довірчих послуг і відповідає вимогам, викладеним у Додатку III;
- (31) "засіб для створення електронної печатки" - налаштоване програмне або апаратне забезпечення, яке використовується для створення електронних печаток;
- (32) "засіб для створення кваліфікованої електронної печатки" - засіб для створення електронної печатки, який відповідає вимогам, викладеним в Додатку II;
- (33) "електронна позначка часу" – дані в електронній формі, які пов'язують інші електронні дані з конкретним моментом часу, встановлюючи доказ того, що ці дані існували в той час;
- (34) "кваліфікована електронна позначка часу" - електронна позначка часу, яка відповідає вимогам, викладеним у статті 42;

- (35) "електронний документ" - будь-який контент, який зберігається в електронній формі, зокрема текст або звук, візуальний або аудіовізуальний запис;
- (36) "послуга рекомендованого електронного відправлення" - послуга, яка дозволяє передавати дані між третіми сторонами за допомогою електронних засобів та надає докази стосовно обробки переданих даних, в тому числі підтвердження передачі та прийому даних, і яка захищає передані дані від ризику втрати, крадіжки, пошкодження або самовільних змін;
- (37) "кваліфікована послуга рекомендованого електронного відправлення" - послуга рекомендованого електронного відправлення, яка відповідає вимогам, викладеним у статті 44;
- (38) "сертифікат для автентифікації веб-сайту" - свідоцтво, що надає можливість автентифікації веб-сайту та пов'язує веб-сайт з фізичною або юридичною особою, якою було отримано сертифікат;
- (39) "кваліфікований сертифікат для автентифікації веб-сайту" - сертифікат для автентифікації веб-сайту, який видається кваліфікованим провайдером довірчих послуг і відповідає вимогам, викладеним в Додатку IV;
- (40) "дані для перевірки достовірності" - дані, які використовуються для перевірки достовірності електронного підпису або електронної печатки;
- (41) "перевірка достовірності" - процес перевірки та підтвердження достовірності електронного підпису або електронної печатки.

Стаття 4

Принцип внутрішнього ринку

1. Не повинно бути жодних обмежень для надання довірчих послуг на території будь-якої держави-члена провайдерами довірчих послуг, заснованими на території інших держав-членів з причин, що належать до сфер, на які розповсюджується дія цього Регламенту.
2. На внутрішньому ринку дозволяється вільний обіг продуктів та довірчих послуг, що відповідають вимогам цього Регламенту.

Стаття 5

Захист та обробка персональних даних

1. Обробка персональних даних здійснюється відповідно до Директиви 95/46/ЄС.
2. Без шкоди для юридичної сили, наданої псевдонімам відповідно до національного законодавства, використання псевдонімів в електронних транзакціях не забороняється.

РОЗДІЛ II

ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ

Стаття 6

Взаємне визнання

1. Коли електронна ідентифікація за допомогою засобів електронної ідентифікації та автентифікації вимагається на підставі національного законодавства або адміністративної практики для доступу до он-лайн послуги, яка надається органом державного сектору на території будь-якої держави-члена, засоби електронної ідентифікації, видані на території іншої держави-члена визнаються першою державою-членом з метою транскордонної автентифікації для цієї он-лайн послуги, за умови виконання наступних вимог:

- (a) засоби електронної ідентифікації видаються за схемою електронної ідентифікації, що міститься в переліку, опублікованому Комісією відповідно до статті 9;

- (b) рівень гарантій цих засобів електронної ідентифікації є відповідним або вищим за рівень гарантій, який вимагає відповідний орган державного сектору для доступу до он-лайн послуги у першій державі-члені, за умови відповідності рівнів гарантій засобів електронної ідентифікації рівню гарантій «суттєвий» або «високий»;
- (c) відповідний орган державного сектору використовує рівень гарантій «суттєвий» або «високий» для доступу до цієї он-лайн послуги.

Таке визнання повинно наступати не пізніше, ніж через 12 місяців після опублікування Комісією переліку, зазначеного в першому абзаці пункту (a).

2. Засоби електронної ідентифікації, які випускаються згідно з схемами електронної ідентифікації, включеними до переліку, опублікованого Комісією відповідно до статті 9, і які відповідають рівню гарантій «низький» можуть бути визнані органами державного сектору з метою забезпечення транскордонної автентифікації для послуг, які надаються цим органом он-лайн.

Стаття 7

Прийнятність для нотифікації схем електронної ідентифікації

Схема електронної ідентифікації є прийнятною в цілях нотифікації на підставі частини 1 статті 9, якщо виконуються всі наступні умови:

- (a) засоби електронної ідентифікації, що належать до схеми електронної ідентифікації, видаються:
 - (i) державою-членом, яка здійснює нотифікацію,
 - (ii) в рамках повноважень держави-члена, яка здійснює нотифікацію, або
 - (iii) незалежно від держави-члена, яка здійснює нотифікацію, але визнаються цією державою-членом;
- (b) засоби електронної ідентифікації, що належать до схеми електронної ідентифікації, можуть використовуватись для доступу, принаймні, до однієї послуги, яка надається органом державного сектору і вимагає електронної ідентифікації на території держави-члена, що здійснює нотифікацію;
- (c) схема та засоби електронної ідентифікації, які видаються відповідно до неї, відповідають вимогам, принаймні, одного з рівнів гарантій, викладених у виконавчому акті, зазначеному в частині 3 статті 8;
- (d) держава-член, що здійснює нотифікацію, стежить за тим, щоб дані персональної ідентифікації, які однозначно представляють зазначену особу, присвоювались зазначеній в пункті 1 статті 3 фізичній або юридичній особі в момент видачі передбаченого цією схемою засобу електронної ідентифікації відповідно до технічних вимог, стандартів та процедур для зазначеного рівня гарантій, передбачених виконавчим актом, зазначеним в частині 3 статті 8;
- (e) сторона, яка видає засоби електронної ідентифікації, що належать до цієї схеми, стежить за тим, щоб засоби електронної ідентифікації закріплювались за зазначеною в пункті (d) цієї статті особою відповідно до технічних вимог, стандартів та процедур для зазначеного рівня гарантій, передбачених виконавчим актом, зазначеним в частині 3 статті 8;
- (f) держава-член, що здійснює нотифікацію, забезпечує доступність он-лайн нотифікації у такий спосіб, щоб будь-яка сторона-користувач, заснована на території іншої держави-члена, могла підтвердити отримані в електронному вигляді дані персональної ідентифікації.

Для сторін-користувачів відмінних від органів державного сектору, держава-член, яка здійснює нотифікацію, може визначати умови доступу до такої автентифікації. Така транскордонна автентифікація здійснюється безкоштовно, якщо вона проводиться у зв'язку з он-лайн послугою, що надається органом державного сектору.

Держави-члени не повинні висувати жодних специфічних диспропорційних технічних вимог до сторін-користувачів, які мають намір здійснювати таку автентифікацію, якщо такі вимоги заважають або значною мірою перешкоджають сумісності нотифікованих схем електронної ідентифікації;

(g) щонайменше за шість місяців до нотифікації схеми електронної ідентифікації відповідно до частини 1 статті 9 держава-член, яка здійснює нотифікацію, доводить до відома інших держав-членів з метою виконання зобов'язань, визначених в частині 5 статті 12, опис схеми відповідно до процесуальних умов, зазначених в частині 6 статті 12.

(h) ця схема відповідає вимогам виконавчого акту, зазначеного в частині 8 статті 12.

Стаття 8

Рівні гарантій схем електронної ідентифікації

1. Схема електронної ідентифікації, нотифікована відповідно до частини 1 статті 9, повинна встановлювати такі рівні гарантій для засобів електронної ідентифікації, що випускаються відповідно до цієї схеми: низький, суттєвий та/або високий.

2. Низький, суттєвий або високий рівень гарантій повинні відповідати наступним критеріям:

- (a) низький рівень гарантії повинен відноситись до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, які забезпечують обмежений ступінь довіри до заявленої або стверджуваної ідентифікаційної інформації про будь-яку особу, та характеризується на основі технічних специфікацій, пов'язаних з ними стандартів та процедур, враховуючи технічні перевірки, мета яких полягає у зменшенні ризику зловживання або підміни ідентифікаційної інформації;
- (b) суттєвий рівень гарантії повинен відноситись до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, які забезпечують суттєвий ступінь довіри до заявленої або стверджуваної ідентифікаційної інформації про будь-яку особу, та характеризується на основі технічних специфікацій, пов'язаних з ними стандартів та процедур, враховуючи технічні перевірки, мета яких полягає у зменшенні ризику зловживання або підміни ідентифікаційної інформації;
- (c) високий рівень гарантії повинен відноситись до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, які забезпечують вищий ступінь довіри до заявленої або стверджуваної ідентифікаційної інформації про будь-яку особу, ніж засіб електронної ідентифікації, що має суттєвий рівень довіри, та характеризується на основі технічних специфікацій, пов'язаних з ними стандартів та процедур, враховуючи технічні перевірки, мета яких полягає у зменшенні ризику зловживання або підміни ідентифікаційної інформації;

3. До 18 вересня 2015 року, враховуючи належні міжнародні стандарти та при дотриманні положень частини 2, Комісія шляхом прийняття виконавчих актів встановлює мінімальні технічні вимоги, стандарти та процедури, на основі яких визначаються слабкий, суттєвий та високий рівні гарантій для засобів електронної ідентифікації в цілях частини 1.

Ці мінімальні технічні вимоги, стандарти та процедури повинні бути встановлені на основі надійності та якості наступних складових:

- (a) процедур доведення та перевірки ідентифікаційної інформації щодо фізичних або юридичних осіб, які подали заявки на видачу їм засобів електронної ідентифікації;

- (b) порядку видачі запитуваних засобів електронної ідентифікації;
- (c) механізму автентифікації, шляхом використання якого фізична або юридична особа використовує засіб електронної ідентифікації для підтвердження стороні-користувачу своєї ідентифікаційної інформації;
- (d) підрозділу, який видає засоби електронної ідентифікації
- (e) будь-якого іншого органу, який бере участь в обробці заявки на видачу засобів електронної ідентифікації; та
- (f) технічних характеристик та характеристик безпеки виданих засобів електронної ідентифікації.

Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 9

Нотифікація

1. Держави-члени, що здійснюють нотифікацію, повідомляють Комісії наступну інформацію, а також подальші зміни, внесені до зазначеної інформації у найкращі строки:

- (a) опис схеми електронної ідентифікації, включаючи її рівні гарантії та виробника(ів) засобів електронної ідентифікації для цієї схеми;
- (b) відповідний наглядний режим та інформацію про режим відповідальності щодо:
 - (i) сторони, яка видає засоби електронної ідентифікації, та
 - (ii) сторони, яка забезпечує процедуру автентифікації.
- (c) орган або органи, відповідальні за схему електронної ідентифікації;
- (d) інформацію про суб'єкта або суб'єктів, які проводять реєстрацію унікальних персональних ідентифікаційних даних;
- (e) опис того, як виконуються вимоги виконавчого акту, зазначеного в частині 8 статті 12;
- (f) опис автентифікації, зазначеної в пункті (f) статті 7;
- (g) порядок зупинення дії або відкликання нотифікованої схеми ідентифікації, або автентифікації, або їх відповідних порушених частин.

2. Через один рік після початку застосування виконавчих актів, зазначених у частині 3 статті 8 та частині 8 статті 12, Комісія повинна опублікувати в *Офіційному віснику Європейського Союзу* перелік схем електронної ідентифікації, що були нотифіковані на підставі частини 1, та основну пов'язану з цим інформацію.

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

4. Держава-член може подати до Комісії запит на видалення власної схеми ідентифікації з переліку, зазначеного в частині 2. Комісія повинна опублікувати в *Офіційному віснику Європейського Союзу* відповідні зміни в переліку протягом одного місяця з дня отримання запиту держави-члена.
5. Комісія може, шляхом запровадження виконавчих актів, визначити обставини, формати і процедури для нотифікації, зазначеної в частині 1. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 10

Порушення безпеки

1. Якщо схема електронної ідентифікації, нотифікована відповідно до частини 1 статті 9 або автентифікація, зазначена в пункті (f) статті 7 є повністю порушеною або частково зміненою у такий спосіб, що це впливає на надійність транскордонної автентифікації цієї схеми, держава-член, яка здійснила нотифікацію, повинна призупинити або невідкладно відкликати транскордонну автентифікацію або її частково змінені частини та поінформувати про це інші держави-члени та Комісію.
2. Якщо порушення або часткова зміна, зазначені в частині 1, були усунуті, держава-член, яка здійснила нотифікацію, повинна поновити транскордонну автентифікацію та невідкладно поінформувати про це інші держави-члени та Комісію.
3. Якщо порушення або часткова зміна, зазначені в пункті 1 не були усунуті протягом 3 місяців після призупинення дії або відкликання схеми, держава-член, яка здійснила нотифікацію, повинна повідомити про скасування схеми електронної ідентифікації інші держави-члени та Комісію.

Комісія повинна невідкладно опублікувати в *Офіційному віснику Європейського Союзу* відповідні зміни до переліку, зазначеного в частині 2 статті 9.

Стаття 11

Відповідальність

1. Держава-член, що здійснює нотифікацію, повинна нести відповідальність за шкоду будь-якій фізичній або юридичній особі, заподіяну навмисно або з необережності через недотримання в транскордонній транзакції зобов'язань, визначених у пунктах (d) та (f) статті 7.
2. Сторона, яка видає засоби електронної ідентифікації, повинна нести відповідальність за шкоду будь-якій фізичній чи юридичній особі, заподіяну навмисно або з необережності через недотримання в транскордонній транзакції зобов'язань, визначених у пункті (e) статті 7.
3. Сторона, яка управляє процедурою автентифікації, повинна нести відповідальність за шкоду будь-якій фізичній чи юридичній особі, заподіяну навмисно або з необережності через нездатність забезпечити в транскордонній транзакції коректних операцій щодо автентифікації, визначених у пункті (f) статті 7.
4. Частини 1, 2 та 3 повинні застосовуватись відповідно до національних положень в сфері відповідальності.
5. Частини 1, 2 та 3 діють без шкоди для відповідальності, яка на підставі національного права покладається на сторони транзакції, здійсненої за допомогою засобів електронної ідентифікації, що належать до нотифікованої схеми електронної ідентифікації на підставі частини 1 статті 9.

Стаття 12

Співпраця та сумісність

1. Національні схеми електронної ідентифікації, нотифіковані відповідно до статті 9, повинні бути сумісними.

2. В цілях частини 1 належить запровадити систему взаємодії.

3. Система взаємодії повинна відповідати таким критеріям:
 - (a) вона має на меті технологічну нейтральність і не повинна допускати дискримінації будь-яких національних технічних рішень електронної ідентифікації в межах держави-члена;
 - (b) вона повинна, в міру можливого, відповідати європейським та міжнародним стандартам;
 - (c) вона повинна сприяти реалізації принципу конфіденційності під час розробки;
 - (d) вона повинна забезпечувати обробку персональних даних відповідно до Директиви 95/46/ЄС.
4. Система взаємодії повинна складатися із:
 - (a) посилань на мінімальні технічні вимоги, пов'язані з рівнями гарантій відповідно до статті 8;
 - (b) таблиці відповідності між національними рівнями гарантій нотифікованих схем електронної ідентифікації та рівнями гарантій, зазначеними в статті 8;
 - (c) посилань на мінімальні технічні вимоги щодо сумісності;
 - (d) посилань на мінімальні блоки ідентифікаційних даних, які однозначно визначають фізичну або юридичну особу, та які доступні у схемах електронної ідентифікації;
 - (e) правил здійснення процедур;
 - (f) положень для врегулювання спорів;
 - (g) спільних експлуатаційних стандартів безпеки.
5. Держави-члени повинні співпрацювати з наступних питань:
 - (a) сумісності схем електронної ідентифікації, нотифікованих відповідно до частини 1 статті 9 та електронних схем ідентифікації, які держави-члени мають намір нотифікувати;
 - (b) безпеки схем електронної ідентифікації.
6. Співробітництво між державами-членами повинно складатися з:
 - (a) обміну інформацією, досвідом і передовою практикою щодо схем електронної ідентифікації, зокрема щодо технічних вимог, пов'язаних з рівнем сумісності та гарантій;
 - (b) обміну інформацією, досвідом і передовою практикою щодо роботи з рівнями гарантій схем електронної ідентифікації відповідно до статті 8;
 - (c) експертної оцінки порушень у схемах електронної ідентифікації, на які розповсюджується дія цього Регламенту;
 - (d) експертизи відповідних розробок у сфері електронної ідентифікації.

7. До 18 березня 2015 року Комісія повинна встановити, шляхом прийняття виконавчих актів, процесуальні умови сприяння співробітництву між державами-членами, про яке йдеться в частинах 5 та 6, з метою досягнення високого рівня довіри і безпеки з урахуванням ступенів ризику.

8. До 18 вересня 2015 року, для встановлення єдиних умов впровадження вимог відповідно до частини 1, Комісія, з урахуванням критеріїв, викладених у частині 3, та беручи до уваги результати співпраці між державами-членами, повинна прийняти виконавчі акти щодо системи взаємодії, як це визначено в частині 4.

9. Виконавчі акти, зазначені в частинах 7 та 8 цієї статті, повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

РОЗДІЛ III

ДОВІРЧІ ПОСЛУГИ

СЕКЦІЯ 1

Загальні положення

Стаття 13

Відповідальність і тягар доказування

1. Без шкоди для положень частини 2, провайдери довірчих послуг повинні нести відповідальність за збиток, заподіяний навмисно або з недбалості будь-якій фізичній або юридичній особі в результаті недотримання зобов'язань, передбачених цим Регламентом.

Тягар доказування умислу або недбалості некваліфікованого провайдера довірчих послуг повинен лягати на фізичну або юридичну особу, яка стверджує про збиток, зазначений у цьому абзаці.

Умисел або недбалість кваліфікованого провайдера довірчих послуг, вважається доведеним поки кваліфікований провайдер довірчих послуг не доведе, що збиток, зазначений у першому абзаці, стався без умислу або недбалості цього кваліфікованого провайдера довірчих послуг.

2. Якщо провайдери довірчих послуг належним чином інформували своїх клієнтів заздалегідь про обмеження на використання наданих ними послуг, і ці обмеження мають бути ідентифіковані третіми сторонами, провайдери довірчих послуг не несуть відповідальності за збитки, які виникли в результаті використання послуг із перевищенням зазначених обмежень.

3. Частини 1 і 2 застосовуються відповідно до національних норм в сфері відповідальності.

Стаття 14

Міжнародні аспекти

1. Довірчі послуги, які надаються провайдерами довірчих послуг, заснованими у третіх країнах, повинні визнаватися юридично еквівалентними довірчим послугам, які надаються кваліфікованими провайдерами довірчих послуг Союзу, якщо довірчі послуги, які мають походження з третіх країн, визнаються відповідно до угоди, укладеної між Союзом і третіми країнами або міжнародними організаціями відповідно до статті 218 Договору про функціонування Європейського Союзу.

2. Угоди, зазначені в частині 1, повинні гарантувати, зокрема, що:
- (а) вимоги, що застосовуються до кваліфікованих провайдерів довірчих послуг, заснованих на території Європейського Союзу, та до кваліфікованих послуг, які ними надаються, виконуються провайдерами довірчих послуг третіх країн або міжнародних організацій, з якими укладено угоди, а також виконуються по відношенню до послуг, які ними надаються;
 - (б) кваліфіковані довірчі послуги, які надаються кваліфікованими провайдерами довірчих послуг, заснованими на території Європейського Союзу, визнаються юридично еквівалентними довірчим послугам, які надаються провайдерами довірчих послуг в третій країні чи міжнародній організації, з якими укладено угоди.

Стаття 15

Доступність для осіб з обмеженими можливостями

В міру можливого довірчі послуги та кінцеві споживчі продукти, що використовуються при наданні цих послуг, повинні бути доступні для осіб з обмеженими можливостями.

Стаття 16

Санкції

Державами-членами закріплюється порядок накладення санкцій, що застосовуються до порушень цього Регламенту. Передбачені санкції повинні бути ефективними, пропорційними та переконливими.

СЕКЦІЯ 2

Нагляд

Стаття 17

Наглядовий орган

1. Держави-члени повинні призначити наглядовий орган, заснований на їх території або, за взаємною домовленістю з іншою державою-членом, наглядовий орган, заснований в цій іншій державі-члені, повинен бути відповідальним за наглядові завдання у вказаній державі-члені.

Наглядовим органам повинні бути надані необхідні повноваження та відповідні ресурси для виконання їхніх завдань.

2. Держави-члени повинні повідомити Комісії назви та адреси їх відповідно призначених наглядових органів.

3. Роль наглядового органу має бути такою:

- (а) контроль кваліфікованих провайдерів довірчих послуг, заснованих на території визначеної держави-члена, шляхом прогнозування та наглядової діяльності, здійснюваної постфактум, для набуття впевненості, що провайдери та кваліфіковані довірчі послуги, які надаються ними, відповідають вимогам, викладеним в цьому Регламенті;
- (б) вжиття заходів, у разі потреби, по відношенню до некваліфікованих провайдерів довірчих послуг, заснованих на території визначеної держави-члена, шляхом наглядової діяльності, здійснюваної постфактум, після отримання інформації про те, що провайдери та довірчі послуги, які надаються ними, можливо не відповідають вимогам, викладеним в цьому Регламенті.

4. В цілях частини 3 та з урахуванням передбачених в ній обмежень завдання наглядового органу включають зокрема:

- (a) співпрацю з іншими наглядовими органами та надання допомоги цим органам відповідно до статті 18;
- (b) аналіз звітів з оцінки відповідності, зазначених в частині 1 статті 20 та частині 1 статті 21;
- (c) інформування інших наглядових органів та громадськості про порушення безпеки або втрати цілісності відповідно до частини 2 статті 19;
- (d) подання до Комісії звіту про його основну діяльність відповідно до частини 6 цієї статті;
- (e) здійснення аудиту або подання запиту до органу з оцінки відповідності щодо проведення оцінки відповідності кваліфікованого провайдера довірчих послуг відповідно до частини 2 статті 20;
- (f) співпрацю з органами з питань захисту даних, зокрема, шляхом їх негайного інформування про результати аудитів кваліфікованих провайдерів довірчих послуг, якщо під час проведення останніх було виявлено порушення правил захисту персональних даних;
- (g) надання провайдерам довірчих послуг та послугам, які вони надають, статусу кваліфікованих та скасування цього статусу відповідно до статей 20 та 21;
- (h) інформування органу, відповідального за національний довірчий список відповідно до частини 3 статті 22 відносно своїх рішень про надання або скасування статусу кваліфікованого, якщо цей орган сам не є наглядовим органом;
- (i) перевірка наявності і правильного застосування положень планів припинення діяльності у випадках припинення діяльності кваліфікованих провайдерів довірчих послуг, у тому числі щодо доступності до інформації, що зберігається, відповідно до пункту (h) частини 2 статті 24;
- (j) вимогу від провайдерів довірчих послуг усунення будь-яких порушень у виконанні вимог цього Регламенту.

5. Держави-члени можуть передбачати, що наглядовий орган повинен встановлювати, підтримувати і оновлювати довірчу інфраструктуру відповідно до умов, встановлених національним законодавством.

6. Щорічно, до 31 березня, кожний наглядовий орган повинен подати до Комісії звіт про основні напрямки діяльності за попередній календарний рік разом з резюме про отримані від провайдерів довірчих послуг нотифікації про порушення відповідно до частини 2 статті 19.

7. Комісія повинна забезпечити доступність річного звіту, зазначеного в частині 6, для всіх держав-членів.

8. Комісія може, шляхом запровадження виконавчих актів, визначити формати і процедури для звіту, зазначеного в частині 6. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

*Стаття 18***Взаємна допомога**

1. Наглядові органи повинні співпрацювати з метою обміну передовою практикою.

Наглядовий орган, на підставі обґрунтованого запиту від іншого наглядового органу, повинен надати цьому органу допомогу таким чином, щоб їхня діяльність здійснювалась узгоджено. Взаємна допомога може охоплювати, зокрема, інформаційні запити і наглядові заходи, такі як запити на проведення перевірок, що пов'язані зі звітами оцінки відповідності, зазначеними у статтях 20 та 21.

2. Наглядовий орган, якому направлено запит про допомогу, може відхилити цей запит за будь-якої з наступних умов:

- (a) наглядовий орган не компетентний у наданні запитуваної допомоги;
- (b) запитувана допомога не пропорційна наглядовій діяльності наглядового органу, яка здійснюється відповідно до статті 17;
- (c) надання запитуваної допомоги є несумісним з цим Регламентом.

3. У разі необхідності держави-члени можуть уповноважити свої відповідні наглядові органи здійснювати спільні розслідування із залученням співробітників наглядових органів інших держав-членів. Домовленості і процедури для таких спільних заходів повинні бути узгоджені і впроваджені відповідно до національного законодавства держав-членів.

*Стаття 19***Вимоги щодо безпеки, що застосовуються до провайдерів довірчих послуг**

1. Кваліфіковані і некваліфіковані провайдери довірчих послуг повинні вжити відповідних технічних та організаційних заходів з управління ризиками, що пов'язані із безпекою довірчих послуг, які вони надають. Беручи до уваги останні технічні досягнення, ці заходи повинні гарантувати, що рівень гарантії пропорційно відповідає ступеню ризику. Зокрема, повинні бути вжиті заходи для запобігання й мінімізації наслідків інцидентів в галузі безпеки, та інформування зацікавлених сторін про негативні наслідки будь-яких інцидентів.

2. Кваліфіковані і некваліфіковані провайдери довірчих послуг негайно та в будь-якому випадку не пізніше ніж через 24 години після того, як їм це стало відомо, повідомляють наглядовий орган та, в разі необхідності, інші відповідні органи, такі як компетентний національний орган із захисту інформації або орган із захисту персональних даних, про будь-які порушення безпеки або втрату цілісності, які мають істотний вплив на довірчі послуги, що надаються або на персональні дані, що використовуються.

Якщо порушення безпеки або втрата цілісності можуть ймовірно негативно вплинути на фізичну або юридичну особу, якій була надана довірна послуга, провайдер довірчої послуги також повинен негайно повідомити фізичну або юридичну особу про таке порушення або втрату цілісності.

За необхідності, зокрема, якщо порушення безпеки або втрата цілісності стосується двох або більше держав-членів, уповноважений наглядовий орган має поінформувати наглядові органи в інших зацікавлених державах-членах та Європейське агентство з мережевої та інформаційної безпеки.

Уповноважений наглядовий орган повинен інформувати громадськість або вимагати від провайдера довірчих послуг зробити це, якщо орган визнає, що розкриття порушення безпеки або втрати цілісності стосується суспільних інтересів.

3. Уповноважений наглядовий орган повинен надавати Європейському агентству з мережевої та інформаційної безпеки один раз на рік звіт щодо повідомлень про порушення, отриманий від провайдерів довірчих послуг.

4. Комісія, шляхом прийняття виконавчих актів, може визначити:
 - (a) подальшу специфікацію заходів, зазначених в частині 1, та
 - (b) формати і процедури, в тому числі кінцеві строки, що стосуються цілей, визначених в частині 2.

Ці виконавчі акти повинні прийматись відповідно до процедури, зазначеної в частині 2 статті 48.

СЕКЦІЯ 3

Кваліфіковані довірчі послуги

Стаття 20

Нагляд за кваліфікованими провайдерами довірчих послуг

1. Кваліфіковані провайдери довірчих послуг повинні щонайменше кожні 24 місяці, за рахунок власних коштів проходити аудит з боку органу з оцінки відповідності для підтвердження того, що вони та кваліфіковані довірчі послуги, які ними надаються, відповідають вимогам, встановленим цим Регламентом, та повинні надавати звіт з оцінки відповідності не пізніше трьох робочих днів після його отримання до наглядового органу.
2. Без відміни положень частини 1, наглядовий орган може в будь-який час провести аудит або надати запит до органу оцінки відповідності щодо проведення оцінки відповідності кваліфікованих провайдерів довірчих послуг за їх власний рахунок для підтвердження того, що вони та кваліфіковані довірчі послуги, які ними надаються, задовольняють умовам, встановленим цим Регламентом. Наглядовий орган повинен повідомити органи з питань захисту даних про результати аудитів, якщо під час їх проведення було виявлено порушення правил захисту персональних даних.
3. У разі, коли наглядовий орган вимагає від кваліфікованого провайдера довірчих послуг усунення порушень вимог, встановлених цим Регламентом, але цей провайдер не виконує відповідних дій в строки, встановлені, в разі необхідності, наглядовим органом, наглядовий орган з урахуванням масштабів, тривалості та наслідків цього невиконання, може відмінити статус кваліфікованого щодо цього провайдера або щодо враженої послуги, яка надавалась провайдером, та інформувати орган, зазначений в частині 3 статті 22 в цілях оновлення списків довіри, зазначених в частині 1 статті 22. Наглядовий орган інформує кваліфікованого провайдера довірчих послуг про скасування його статусу кваліфікованого, або статусу кваліфікованого щодо конкретної послуги.
4. Комісія може, шляхом запровадження виконавчих актів, визначити перелік наступних стандартів:
 - (a) стандарти щодо акредитації органів з оцінки відповідності, а також щодо звіту з оцінки відповідності, про які йдеться в частині 1;
 - (b) стандарти щодо правил аудиту, за яких органи з оцінки відповідності будуть здійснювати оцінку відповідності кваліфікованих провайдерів довірчих послуг, про які йдеться в частині 1.

Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

*Стаття 21***Запуск кваліфікованої довірчої послуги**

1. У випадку, якщо провайдер довірчих послуг, який не має статусу кваліфікованого, має намір надавати кваліфіковані довірчі послуги, він повинен повідомити наглядовий орган про свій намір та надати звіт з оцінки відповідності, виданий органом з оцінки відповідності.

2. Наглядовий орган повинен перевірити провайдера довірчих послуг та довірчі послуги, які ним надаються на відповідність вимогам цього Регламенту, зокрема вимогам, встановленим для кваліфікованих провайдерів довірчих послуг та для кваліфікованих довірчих послуг, які ними надаються.

Якщо наглядовий орган робить висновок, що провайдер довірчих послуг і довірчі послуги, які ним надаються, задовольняють цим вимогам, наглядовий орган повинен надати провайдеру довірчих послуг статус кваліфікованого та інформувати орган, зазначений в частині 3 статті 22 про необхідність внесення змін до довірчих списків, зазначених в частині 1 статті 22, не пізніше ніж через три місяці після повідомлення, зазначеного в частині 1.

Якщо перевірку не буде завершено протягом трьох місяців, наглядовий орган повинен інформувати провайдера довірчих послуг із зазначенням причин затримки та період, протягом якого перевірку повинно бути завершено.

3. Кваліфіковані провайдери довірчих послуг можуть почати надавати кваліфіковану довірчу послугу після того, як інформацію про статус, буде внесено до довірчих списків, зазначених в частині 1 статті 22.

4. Комісія може, шляхом запровадження виконавчих актів, визначити формати і процедури, необхідні для досягнення цілей, зазначених в частинах 1 та 2. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

*Стаття 22***Довірчі списки**

1. Кожна держава-член розробляє, веде та опубліковує довірчі списки, враховуючи інформацію про кваліфікованих провайдерів довірчих послуг, за яких вона несе відповідальність, а також інформацію про кваліфіковані довірчі послуги, що ними надаються.

2. Держави-члени розробляють, ведуть та опубліковують у безпечний спосіб та в формі, адаптованій для автоматичної обробки, зазначені в частині 1 довірчі списки, що містять електронний підпис або електронну печатку.

3. Держави-члени невідкладно повідомляють Комісії інформацію про орган, уповноважений на розробку, ведення та опублікування національних довірчих списків, а також докладну інформацію щодо того де ці списки опубліковано із зазначенням сертифікатів, використаних для проставлення електронного підпису або електронної печатки на зазначені списки та попередженням про будь-які, внесені до цих списків, зміни.

4. Комісія, шляхом використання захищеного каналу зв'язку, повинна зробити доступною для громадськості інформацію, зазначену в частині 3, в формі, що містить електронний підпис або електронну печатку та є адаптованою для автоматичної обробки.

5. До 18 вересня 2015 року Комісія уточнює, шляхом використання виконавчих актів, зазначену в частині 1 інформацію та визначає технічні специфікації і формати для довірчих списків, що застосовуються в цілях частин 1-4. Ці виконавчі акти ухвалюються відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 23

Знак довіри ЄС для кваліфікованих довірчих послуг

1. Після того, як статус кваліфікованого, зазначений в другому абзаці частини 2 статті 21, був внесений в довірчий список, зазначений в частині 1 статті 22, кваліфіковані провайдери довірчих послуг можуть використовувати знак довіри ЄС для зазначення у простий, зрозумілий та прозорий спосіб того, які довірчі послуги вони надають.
2. Під час використання для кваліфікованих довірчих послуг знаку довіри ЄС, зазначеного в частині 1, кваліфіковані провайдери довірчих послуг повинні забезпечити доступність посилання на відповідний довірчий список на їхньому сайті.
3. До 1 липня 2015 Комісія має, шляхом запровадження виконавчих актів, прийняти специфікації щодо форми та, зокрема, вигляду, складу, розміру та дизайну знаку довіри ЄС для кваліфікованих довірчих послуг. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 24

Вимоги до кваліфікованих провайдерів довірчих послуг

1. Під час видачі кваліфікованого сертифіката для довірчої послуги, провайдер кваліфікованих довірчих послуг за допомогою відповідних засобів та відповідно до національного законодавства, перевіряє ідентифікаційні дані та, в разі необхідності, всі спеціальні характеристики фізичної або юридичної особи, якій він видає кваліфікований сертифікат.

Інформація, про яку йдеться у попередньому абзаці, повинна бути перевірена кваліфікованим провайдером довірчих послуг або безпосередньо ним, або шляхом звернення до третьої сторони на підставі національного законодавства.

- (a) за умови фізичної присутності фізичної особи або уповноваженого представника юридичної особи, або
 - (b) дистанційно, з використанням засобів електронної ідентифікації в разі, якщо раніше для видачі кваліфікованого сертифіката було забезпечено фізичну присутність фізичної особи або уповноваженого представника юридичної особи та, якщо виконані вимоги, встановлені відповідно до статті 8 щодо рівнів гарантій "суттєвий" або "високий", або
 - (c) за допомогою сертифіката кваліфікованого електронного підпису або кваліфікованої електронної печатки, виданих відповідно до пункту (a) або (b), або
 - (d) за допомогою інших методів ідентифікації, визнаних на національному рівні, які забезпечують еквівалентної гарантії фізичної присутності. Еквівалентна гарантія повинна бути підтверджена органом з оцінки відповідності.
2. Кваліфіковані провайдери довірчих послуг при наданні кваліфікованих довірчих послуг повинні:
 - (a) інформувати наглядовий орган про будь-які зміни в наданні кваліфікованих довірчих послуг, в тому числі про намір припинити свою діяльність;
 - (b) наймати персонал і, в разі необхідності, субпідрядників, які володіють необхідним професіоналізмом, надійністю, досвідом та кваліфікацією, та які отримали відповідну підготовку щодо дотримання правил безпеки та захисту персональних даних, та застосовують адміністративні та управлінські процедури, які відповідають європейським або міжнародним стандартам
 - (c) що стосується ризику відповідальності за шкоду, про яку йдеться у статті 13, підтримувати достатні фінансові ресурси та/або оформити відповідне страхування цивільної відповідальності згідно з національним законодавством;

- (d) до набуття договірних відносин, у прозорий та всебічний спосіб повідомляти будь-яку особу, що прагне використовувати кваліфіковану довірчу послугу, про чіткі строки та умови використання цієї послуги, у тому числі про будь-які обмеження в її використанні;
- (e) використовувати надійні системи і продукти, які захищені від модифікації і гарантують технічну безпеку і надійність процесу, що ними підтримується;
- (f) використовувати надійні системи для зберігання даних, наданих їм у формі, придатній для перевірки, таким чином, щоб:
 - (i) вони були доступними для пошуку тільки у випадку згоди особи, до якої належать ці дані,
 - (ii) тільки уповноважені особи могли робити записи і зміни у даних, що зберігаються,
 - (iii) дані можна було перевірити на достовірність;
- (g) вжити відповідних заходів проти підробки і крадіжки даних;
- (h) записувати та забезпечувати доступність протягом відповідного періоду часу, у тому числі після припинення кваліфікованим провайдером довірчих послуг його діяльності, всю необхідну інформацію про дані, видані та отримані провайдером кваліфікованих довірчих послуг, зокрема, з метою надання доказів у судовому розгляді та для забезпечення безперервності надання послуг. Такий запис може бути зроблений в електронному вигляді;
- (i) мати план припинення діяльності, який відповідає сучасним вимогам, для забезпечення безперервності обслуговування відповідно до погоджених із наглядовим органом положень, зазначених у пункті (i) частини 4 статті 17;
- (j) забезпечити законну обробку персональних даних відповідно до Директиви 95/46/ЄС;
- (i) впровадити й забезпечити підтримку оновленої бази даних сертифікатів кваліфікованими провайдерами довірчих послуг, які видають кваліфіковані сертифікати,

3. Якщо кваліфіковані провайдери довірчих послуг, які видають кваліфіковані сертифікати, прийняли рішення відкликати сертифікат, вони повинні зареєструвати таке відкликання в базі даних сертифікатів та вчасно опублікувати статус відкликаноного сертифіката, але в будь-якому випадку протягом 24 годин після отримання запиту. Таким чином відкликання набирає чинності негайно після відповідного опублікування.

4. Що стосується частини 3, провайдери кваліфікованих довірчих послуг, які видають кваліфіковані сертифікати, повинні надати будь-якій стороні-користувачу інформацію про чинність або статус відкликання виданих ними кваліфікованих сертифікатів. Ця інформація повинна бути доступна в будь-який час протягом строку чинності сертифікату, принаймні на основі сертифікатів, в автоматичному режимі, який є надійним, безкоштовним і ефективним.

5. Комісія, шляхом прийняття виконавчих актів, може встановити перелік стандартів для надійних систем і продуктів, які відповідають вимогам, зазначеним у підпунктах (e) та (f) частини 2 цієї статті. Дотримання вимог, викладених у статті 24, вважається досягнутим, якщо надійні системи та продукти відповідають цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

СЕКЦІЯ 4

Електронні підписи*Стаття 25***Юридична сила електронних підписів**

1. Електронний підпис не може бути позбавлений юридичної сили і можливості розглядатись як доказ у судових справах виключно на тій підставі, що він має електронний вигляд або не відповідає вимогам до кваліфікованого електронного підпису.
2. Кваліфікований електронний підпис повинен мати таку ж юридичну силу як і власноручний підпис.
3. Кваліфікований електронний підпис, заснований на кваліфікованому сертифікаті, який виданий в одній державі-члені повинен визнаватись як кваліфікований електронний підпис у всіх інших державах-членах.

*Стаття 26***Вимоги до удосконалених електронних підписів**

Удосконалений електронний підпис повинен відповідати таким вимогам:

- (a) бути однозначно пов'язаним з підписувачем;
- (b) надавати можливість ідентифікувати підписувача;
- (c) створюватись з використанням даних для створення електронного підпису, які підписувач може, з високим ступенем впевненості, одноосібно контролювати;
- (d) бути пов'язаним з підписаними даними таким чином, що будь-яка наступна зміна даних може бути виявлена.

*Стаття 27***Електронні підписи для державних послуг**

1. Якщо держава-член вимагає використання удосконаленого електронного підпису для он-лайн послуг, які надаються органом державного сектору або від його імені, держава-член повинна визнавати удосконалені електронні підписи, удосконалені електронні підписи, засновані на кваліфікованому сертифікаті для електронних підписів, та кваліфіковані електронні підписи принаймні, в форматах або з використанням методів, зазначених в частині 5.
2. Якщо держава-член вимагає використання удосконаленого електронного підпису, заснованого на кваліфікованому сертифікаті для он-лайн послуг, які надаються органом державного сектору або від його імені, держава-член повинна визнавати удосконалені електронні підписи, засновані на кваліфікованому сертифікаті, та кваліфіковані електронні підписи принаймні, в форматах або з використанням методів, зазначених в частині 5.
3. Держави-члени не повинні вимагати для транскордонного використання в он-лайн послугах, які пропонуються органом державного сектору, електронний підпис із більш високим рівнем безпеки, ніж кваліфікований електронний підпис.
4. Комісія, шляхом прийняття виконавчих актів, може встановити перелік стандартів для удосконалених електронних підписів. Дотримання вимог до удосконалених електронних підписів, зазначених в частинах 1 та 2 цієї статті та в статті 26, вважається досягнутим, якщо удосконалений електронний підпис відповідає цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

5. До 18 вересня 2015 року, та з урахуванням існуючої практики, стандартів та правових актів Союзу, Комісія повинна прийняти виконавчі акти, які визначають відповідні формати удосконалених електронних підписів або еталонних методів, в яких використовуються альтернативні формати. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 28

Кваліфіковані сертифікати електронного підпису

1. Кваліфіковані сертифікати електронного підпису повинні відповідати вимогам, викладеним у Додатку I.
2. До кваліфікованих сертифікатів електронного підпису не повинні висуватися будь-які обов'язкові вимоги, що виходять за межі вимог, викладених у Додатку I.
3. Кваліфіковані сертифікати для електронних підписів можуть включати необов'язкові додаткові спеціальні характеристики. Ці характеристики не повинні впливати на сумісність і визнання кваліфікованих електронних підписів.
4. Якщо кваліфікований сертифікат електронного підпису був відкликаний після початкової активації, то він повинен втрачати свою чинність з моменту його відкликання, а його статус не повинен бути відновленим за жодних обставин.
5. Держави-члени можуть прийняти національні норми відносно тимчасового припинення дії кваліфікованих сертифікатів електронного підпису з урахуванням таких умов:
 - (a) якщо кваліфікований сертифікат електронного підпису був тимчасово заблокований, цей сертифікат повинен втрачати свою чинність на період тимчасового припинення дії.
 - (b) строк тимчасового припинення дії повинен бути чітко вказаний в базі даних сертифікатів, і статус тимчасового припинення дії повинен бути видимим протягом періоду тимчасового припинення дії, шляхом надання службової інформації про статус сертифіката.
6. Комісія, шляхом прийняття виконавчих актів, може встановлювати перелік стандартів для кваліфікованих сертифікатів електронного підпису. Дотримання вимог, викладених у Додатку I, вважається досягнутим, якщо кваліфікований сертифікат електронного підпису відповідає цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 29

Вимоги до засобів для створення кваліфікованого електронного підпису

1. Засоби для створення кваліфікованого електронного підпису повинні відповідати вимогам, викладеним у Додатку II.
2. Комісія, шляхом прийняття виконавчих актів, може встановлювати переліки стандартів для засобів для створення кваліфікованого електронного підпису. Дотримання вимог, викладених у Додатку II, вважається досягнутим, якщо засіб для створення кваліфікованого електронного підпису відповідає цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 30

Сертифікація засобів для створення кваліфікованого електронного підпису

1. Відповідність засобів для створення кваліфікованого електронного підпису вимогам Додатку II повинна бути сертифікована відповідним державним чи приватним органом, що визначається державою-членом.

2. Держави-члени повинні нотифікують Комісії назви та адреси державних або приватних органів, призначених ними відповідно до частини 1. Комісія повинна надати цю інформацію у розпорядження держав-членів.

3. Зазначена в частині 1 сертифікація повинна базуватись на одному з таких процесів:

- (a) процесі оцінки безпеки, запровадженому відповідно до одного з стандартів щодо оцінки безпеки інформаційної продукції, що містяться в переліку, розробленому відповідно до другого абзацу; або
- (b) процесі, відмінному від процесу, зазначеного в пункті (a), за умови, що цей процес використовує зіставні рівні безпеки, а державний або приватний орган, зазначений в частині 1, здійснює нотифікацію цього процесу Комісії. Такий процес може бути використаний лише за відсутності стандартів, зазначених у першому абзаці, або коли процес оцінки безпеки, зазначений у першому абзаці, прийнятний на постійній основі.

Комісія розробляє, шляхом використання виконавчих актів, перелік стандартів щодо оцінки безпеки інформаційних продуктів, зазначених в пункті (a). Ці виконавчі акти ухвалюються відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

4. Комісія уповноважена ухвалювати делеговані акти відповідно до статті 47 щодо встановлення конкретних критеріїв, яким повинні відповідати призначені органи, про які йдеться в частині 1.

Стаття 31

Опублікування списку сертифікованих засобів для створення кваліфікованого електронного підпису

1. Держави-члени повинні повідомити Комісії, без невинуватої затримки та не пізніше 1 місяця з моменту завершення сертифікації, інформацію про засоби для створення кваліфікованого електронного підпису, які були сертифіковані органами, зазначеними в частині 1 статті 30. Вони також повинні повідомити Комісії, без невинуватої затримки та не пізніше 1 місяця з моменту скасування сертифікації, інформацію про засоби для створення електронного підпису, які більше не є сертифікованими.

2. На основі отриманої інформації, Комісія розробляє, опубліковує та оновлює перелік сертифікованих засобів для створення кваліфікованого електронного підпису.

3. Комісія, шляхом прийняття виконавчих актів, може визначати формати і процедури, які будуть застосовуватись для досягнення цілей, зазначених в частині 1. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 32

Вимоги щодо перевірки кваліфікованих електронних підписів

1. Процес перевірки кваліфікованого електронного підпису повинен підтвердити справжність електронного підпису за умови, що:

- (a) сертифікат, на якому засновано підпис, на момент підписання був кваліфікованим сертифікатом електронного підпису та відповідав вимогам, викладеними в Додатку I;
- (b) кваліфікований сертифікат був виданий кваліфікованим провайдером довірчих послуг і був дійсним на момент підписання;
- (c) дані перевірки підпису відповідають даним, повідомленим стороні-користувачу;

- (d) унікальний набір даних, що представляє підписувача у сертифікаті, був коректно наданий стороні-користувачу;
 - (e) використання будь-якого псевдоніма, якщо такий був використаний на момент підписання, чітко зрозуміло стороні-користувачу;
 - (f) електронний підпис створений пристроєм для створення кваліфікованого електронного підпису;
 - (g) цілісність підписаних даних не була порушеною;
 - (h) на момент підписання було виконано вимоги, передбачені статтею 26.
2. Система, яка використовується для перевірки електронного підпису, повинна надавати стороні-користувачу коректний результат процесу перевірки та повинна дозволяти стороні-користувачу виявити всі проблеми, що стосуються безпеки.
3. Комісія, шляхом прийняття виконавчих актів, може визначати перелік стандартів для перевірки кваліфікованого електронного підпису. Дотримання вимог, викладених в частині 1, вважається досягнутим, якщо перевірка кваліфікованого електронного підпису відповідає цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 33

Кваліфікована послуга перевірки кваліфікованих електронних підписів

1. Кваліфікована послуга перевірки кваліфікованих електронних підписів може надаватися лише кваліфікованим провайдером довірчих послуг, який:
- (a) забезпечує перевірку відповідно до частини 1 статті 32 та
 - (b) дозволяє сторонам-користувачам отримувати результат процесу перевірки в автоматичному режимі, що є надійним, ефективним і використовує вдосконалений електронний підпис або електронну печатку провайдера кваліфікованої послуги перевірки.
2. Комісія, шляхом прийняття виконавчих актів, може визначати перелік стандартів для кваліфікованих послуг перевірки, про які йдеться в частині 1. Дотримання вимог, викладених у пункті (b) частини 1, вважається досягнутим, якщо послуга перевірки кваліфікованого електронного підпису відповідає цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 34

Кваліфікована послуга збереження кваліфікованих електронних підписів

1. Кваліфікована послуга збереження кваліфікованих електронних підписів може надаватись лише кваліфікованим провайдером довірчих послуг, який використовує процедури і технології, здатні розширювати надійність кваліфікованого електронного підпису за межі строку технологічного строку дії.
2. Комісія може, шляхом прийняття виконавчих актів, визначати вихідні номери стандартів, що застосовуються для кваліфікованої послуги збереження кваліфікованих електронних підписів. Дотримання вимог, викладених в частині 1, вважається досягнутим, якщо заходи щодо кваліфікованого збереження кваліфікованого електронного підпису відповідають цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

СЕКЦІЯ 5

Електронні печатки*Стаття 35***Юридична сила електронної печатки**

1. Електронну печатку не може бути позбавлено юридичної сили і можливості розглядатись як доказ у судових справах виключно на тій підставі, що вона має електронний вигляд або не відповідає вимогам до кваліфікованої електронної печатки.
2. Кваліфікована електронна печатка повинна користуватись презумпцією цілісності даних і достовірністю походження даних, з якими кваліфікована електронна печатка пов'язана.
3. Кваліфікована електронна печатка, заснована на кваліфікованому сертифікаті, виданому на території однієї держави-члена повинна визнаватись як кваліфікована електронна печатка на території всіх інших державах-членах.

*Стаття 36***Вимоги до удосконалених електронних печаток**

Удосконалена електронна печатка повинна відповідати таким вимогам:

- (a) бути однозначно пов'язаною із розробником печатки;
- (b) надавати можливість ідентифікувати розробника печатки;
- (c) створюватись з використанням даних для створення електронної печатки, які розробник печатки може, з високим ступенем впевненості контролювати та використовувати для створення електронної печатки і
- (d) бути пов'язаною з даними, до яких вона відноситься, таким чином, що будь-яка наступна зміна даних може бути виявлена.

*Стаття 37***Електронні печатки для державних послуг**

1. Якщо держава-член вимагає використання удосконаленої електронної печатки для он-лайн послуг, які надаються органом державного сектору, або від його імені, держава-член повинна визнавати удосконалені електронні печатки, удосконалені електронні печатки, засновані на кваліфікованому сертифікаті для електронних печаток, та кваліфіковані електронні печатки принаймні, в форматах або з використанням методів, зазначених в частині 5.
2. Якщо держава-член вимагає використання удосконаленої електронної печатки, заснованої на кваліфікованому сертифікаті, для он-лайн послуг, які надаються органом державного сектору, або від його імені, держава-член повинна визнавати удосконалені електронні печатки, засновані на кваліфікованому сертифікаті, та кваліфіковані електронні печатки принаймні, в форматах або з використанням методів, зазначених в частині 5.
3. Держави-члени не повинні вимагати для транскордонного використання в он-лайн послугах, які пропонуються органом державного сектору, електронні печатки з більш високим рівнем безпеки, ніж кваліфіковані електронні печатки.
4. Комісія, шляхом прийняття виконавчих актів, може встановити перелік стандартів для удосконалених електронних печаток. Дотримання вимог до удосконалених електронних печаток, зазначених в частинах 1 та 2 цієї статті та в статті 36, вважається досягнутим, якщо удосконалена електронна печатка відповідає цим

стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

5. До 18 вересня 2015 року, та з урахуванням існуючої практики, стандартів та правових актів Європейського Союзу, Комісія повинна прийняти виконавчі акти, які визначають відповідні формати удосконалених електронних печаток або еталонні методи, в яких використовуються альтернативні формати. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 38

Кваліфіковані сертифікати для електронних печаток

1. Кваліфіковані сертифікати для електронної печатки, повинні відповідати вимогам, викладеним у Додатку III.
2. До кваліфікованих сертифікатів електронної печатки не повинні висуватися будь-які обов'язкові вимоги, що перевищують вимоги, викладені в Додатку III.
3. Кваліфіковані сертифікати для електронних печаток можуть включати необов'язкові додаткові спеціальні характеристики. Ці характеристики не повинні впливати на сумісність і визнання кваліфікованих електронних печаток.
4. Якщо кваліфікований сертифікат для електронної печатки був відкликаний після початкової активації, то він повинен втрачати свою чинність з моменту його відкликання, а його статус не повинен бути відновленим за жодних обставин.
5. Держави-члени можуть прийняти національні норми відносно тимчасового припинення дії кваліфікованих сертифікатів для електронної печатки з урахуванням таких умов:
 - (a) якщо кваліфікований сертифікат для електронної печатки був тимчасово заблокований, цей сертифікат повинен втрачати свою чинність на період тимчасового припинення дії.
 - (b) строк тимчасового припинення дії повинен бути чітко вказаний в базі даних сертифікатів, і статус тимчасового припинення дії повинен бути видимим протягом періоду тимчасового припинення дії шляхом надання службової інформації про статус сертифіката.
6. Комісія, шляхом прийняття виконавчих актів, може встановлювати перелік стандартів для кваліфікованих сертифікатів для електронної печатки. Дотримання вимог, викладених у Додатку III, вважається досягнутим, якщо кваліфікований сертифікат для електронної печатки відповідає цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

Стаття 39

Засоби створення кваліфікованої електронної печатки

1. Для визначення вимог до засобів створення кваліфікованої електронної печатки застосовується стаття 29 з відповідними змінами.
2. Для визначення вимог до сертифікації засобів створення кваліфікованої електронної печатки застосовується стаття 30 з відповідними змінами.
3. Для визначення вимог до публікації списку сертифікованих засобів створення кваліфікованої електронної печатки застосовується стаття 31 з відповідними змінами.

Стаття 40

Перевірка та збереження кваліфікованих електронних печаток

Щодо перевірки та збереження кваліфікованих електронних печаток застосовуються статті 32, 33 та 34 з відповідними змінами.

СЕКЦІЯ 6

*Електронна позначка часу**Стаття 41***Юридична сила електронних позначок часу**

1. Електронна позначка часу не може бути позбавлена юридичної сили і можливості розглядатись як доказ у судових справах виключно на тій підставі, що вона має електронний вигляд або не відповідає вимогам до кваліфікованої позначки часу.
2. Кваліфікована електронна позначка часу повинна користуватись презумпцією точності дати та часу, на які вона вказує, та цілісності даних, з якими ці дата та час пов'язані.
3. Кваліфікована електронна позначка часу, видана на території однієї з держав-членів повинна бути визнана як кваліфікована електронна позначка часу на території всіх держав-членів.

*Стаття 42***Вимоги до кваліфікованих позначок часу**

1. Кваліфікована позначка часу повинна відповідати таким вимогам:
 - (a) пов'язувати дату і час з даними в такий спосіб, що цілком виключає можливість непомітної зміни даних;
 - (b) базуватися на точному джерелі часу, пов'язаному з універсальним координованим часом (UTC);
 - (c) бути підписаною за допомогою удосконаленого електронного підпису або містити проставлену удосконалену електронну печатку кваліфікованого провайдера довірчих послуг, або іншим еквівалентним методом.
2. Комісія, шляхом прийняття виконавчих актів, може встановлювати перелік стандартів щодо пов'язання дати та часу із даними та щодо точності джерела часу. Дотримання вимог, викладених в частині 1, вважається досягнутим, якщо прив'язка дати та часу до даних та точність джерела часу відповідають цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

СЕКЦІЯ 7

*Послуги рекомендованих електронних відправлень**Стаття 43***Юридична сила послуги рекомендованого електронного відправлення**

1. Дані, які відправлені та отримані з використанням послуги рекомендованого електронного відправлення, не можуть бути позбавлені юридичної сили і можливості розглядатись як доказ у судових справах виключно на тій підставі, що вони мають електронний вигляд, або не відповідають вимогам до кваліфікованої послуги рекомендованого електронного відправлення.
2. Дані, які відправлені та отримані з використанням кваліфікованої послуги рекомендованого електронного відправлення, повинні користуватись презумпцією цілісності даних, передачі ідентифікованим відправником та отримання ідентифікованим отримувачем даних та точності дати і часу відправки та отримання даних, які зазначаються під час надання кваліфікованої послуги рекомендованого електронного відправлення.

*Стаття 44***Вимоги до кваліфікованої послуги рекомендованого електронного відправлення**

1. Кваліфіковані послуги рекомендованих електронних відправлень повинні відповідати таким вимогам:
 - (a) вони повинні надаватися одним чи кількома кваліфікованими провайдерами довірчих послуг;
 - (b) вони повинні забезпечувати ідентифікацію відправника з високим рівнем довіри;
 - (c) перед доставкою даних, повинна бути забезпечена ідентифікація отримувача;
 - (d) відправка та отримання даних повинні бути захищеними з використанням вдосконаленого електронного підпису або удосконаленої електронної печатки кваліфікованого провайдера довірчих послуг у спосіб, який виключає можливість непоміченої зміни даних;
 - (e) відправник і отримувач даних повинні бути чітко повідомлені про будь-яку зміну даних, необхідну для відправки або отримання даних;
 - (f) дата і час відправки, отримання та будь-яка зміна даних повинні бути позначені за допомогою кваліфікованої електронної позначки часу;

У разі відправки даних між двома або більше кваліфікованими провайдерами довірчих послуг, вимоги пунктів (a) - (f) повинні застосовуватися до всіх кваліфікованих провайдерів довірчих послуг.

2. Комісія, шляхом прийняття виконавчих актів, може встановлювати перелік стандартів щодо процесів відправки та отримання даних. Дотримання вимог, викладених в частині 1, вважається досягнутим, якщо процеси відправки та отримання даних відповідають цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

СЕКЦІЯ 8***Автентифікація веб-сайту****Стаття 45***Вимоги, що застосовуються до кваліфікованих сертифікатів для автентифікації веб-сайту**

1. Кваліфіковані сертифікати для автентифікації веб-сайту повинні відповідати вимогам, викладеним у Додатку IV.
2. Комісія, шляхом прийняття виконавчих актів, може визначити вихідні номери стандартів, що застосовуються кваліфікованих сертифікатів автентифікації веб-сайту. Дотримання вимог, викладених у Додатку IV, вважається досягнутим, якщо кваліфікований сертифікат для автентифікації веб-сайту відповідає цим стандартам. Зазначені виконавчі акти ухвалюються відповідно до процедури експертизи, зазначеної в частині 2 статті 48.

РОЗДІЛ IV**ЕЛЕКТРОННІ ДОКУМЕНТИ***Стаття 46***Юридична сила електронних документів**

Електронний документ не може бути позбавлений юридичної сили і можливості розглядатись як доказ у судових справах виключно на тій підставі, що він має електронний вигляд.

РОЗДІЛ V

ДЕЛЕГУВАННЯ ПОВНОВАЖЕНЬ ТА ВИКОНАВЧІ ПОЛОЖЕННЯ

Стаття 47

Здійснення делегування

1. Надане Комісії повноваження ухвалювати делеговані акти підлягає визначеним цією статтею умовам.
2. Повноваження ухвалювати зазначені в частині 4 статті 30 делеговані акти надається Комісії на невизначений період часу починаючи з 17 вересня 2014 року.
3. Делегування зазначених в частині 4 статті 30 повноважень може бути відкликаним в будь-який час Європейським Парламентом або Радою. Рішення про відкликання має припинити делегування повноважень, зазначених у цьому рішенні. Відкликання набуває чинності наступного дня після опублікування рішення в *Офіційному віснику Європейського Союзу* або з більш пізньої дати, зазначеної у вказаному рішенні. Це не повинно впливати на чинність делегованих актів, що вже є чинними.
4. Одразу після ухвалення делегованого акту, Комісія повинна одночасно офіційно повідомити про нього Європейський Парламент та Раду.
5. Делегований акт, ухвалений на підставі частини 4 статті 30, набуває чинності лише за відсутності заперечень з боку Європейського Парламенту і Ради протягом двох місяців після офіційного повідомлення про цей акт Європейського Парламенту і Ради або, якщо до закінчення цього строку Європейський Парламент і Рада повідомлять Комісію, що вони не мають заперечень. Цей період може бути продовжений на два місяці за ініціативою Європейського Парламенту чи Ради.

Стаття 48

Комітет

1. Комісія працює за сприяння Комітету. Цей комітет є комітетом відповідно до змісту Регламенту (ЄС) № 182/2011.
2. В разі посилання на цю частину -застосовується стаття 5 Регламенту (ЄС) 182/2011.

РОЗДІЛ VI

ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Стаття 49

Перегляд

Комісія здійснює перегляд застосування цього Регламенту та подає звіт Європейському Парламенту та Раді до 1 липня 2020 року. Комісія визначає зокрема чи потрібно змінювати сферу застосування цього Регламенту або його спеціальних положень, враховуючи статтю 6, пункт (f) статті 7 та статті 34, 43, 44 та 45 враховуючи досвід, набутий в процесі застосування цього Регламенту, а також технологічний, ринковий і правовий прогрес.

До зазначеного в першому абзаці звіту в разі необхідності додаються законодавчі пропозиції.

Крім того, Комісія кожні 4 роки після подання зазначеного в першому абзаці звіту подає Європейському Парламенту та Раді звіт щодо успіхів, досягнутих під час реалізації цілей цього Регламенту.

*Стаття 50***Скасування**

1. Директива 1999/93/ЄС скасовується з 1 липня 2016 року.
2. Посилання на скасовану Директиву тлумачаться як посилання на цей Регламент.

*Стаття 51***Перехідні положення**

1. Безпечні засоби створення підпису, відповідність яких було підтверджено відповідно до частини 4 статті 3 Директиви 1999/93/ЄС вважаються засобами для створення кваліфікованого підпису відповідно до цього Регламенту.
2. Кваліфіковані сертифікати, видані для фізичних осіб згідно з Директивою 1999/93/ЄС вважаються кваліфікованими сертифікатами для електронних підписів відповідно до цього Регламенту до закінчення їх строку дії.
3. Провайдер послуг сертифікації, який видає кваліфіковані сертифікати відповідно до Директиви 1999/93/ЄС подає звіт з оцінки відповідності до наглядового органу якомога скоріше, але не пізніше 1 липня 2017 року. До подання такого звіту з оцінки відповідності та завершення його оцінки наглядовим органом цей провайдер послуг сертифікації вважається кваліфікованим провайдером довірчих послуг на підставі цього Регламенту.
4. Якщо провайдер послуг сертифікації, який видає кваліфіковані сертифікати на підставі Директиви 1999/93/ЄС не подасть звіт з оцінки відповідності до наглядового органу протягом строку, зазначеного в частині 3, такий провайдер послуг сертифікації не вважатиметься з 2 липня 2017 року кваліфікованим провайдером довірчих послуг на підставі цього Регламенту.

*Стаття 52***Набрання чинності**

1. Цей Регламент набирає чинності на двадцятий день після його опублікування в *Офіційному віснику Європейського Союзу*.
2. Цей Регламент застосовується з 1 липня 2016, за винятком наступних положень:
 - (a) частини 3 статті 8, частини 5 статті 9, частин 2-9 статті 12, частини 8 статті 17, частини 4 статті 19, частини 4 статті 20, частини 4 статті 21, частини 5 статті 22, частини 3 статті 23, частини 5 статті 24, частин 4 та 5 статті 27, частини 6 статті 28, частини 2 статті 29, частин 3 та 4 статті 30, частини 3 статті 31, частини 3 статті 32, частини 2 статті 33, частини 2 статті 34, частин 4 та 5 статті 37, частини 6 статті 38, частини 2 статті 42, частини 2 статті 44, частини 2 статті 45, та статті 47 та 48 застосовуються з 17 вересня 2014 року;
 - (b) стаття 7, частини 1 та 2 статті 8, статті 9, 10, 11 та частина 1 статті 12, застосовуються з дати прийняття виконавчих актів, зазначених в частині 3 статті 8 та частини 8 статті 12;
 - (c) стаття 6 застосовується через 3 роки з дати прийняття виконавчих актів, зазначених в частині 3 статті 8, а також частині 8 статті 12.
3. Якщо нотифіковану схему електронної ідентифікації включено до переліку, опублікованого Комісією відповідно до статті 9 до дати, зазначеної в пункті (c) частини 2 цієї статті, визнання засобів електронної ідентифікації цієї схеми відповідно до статті 6 повинно відбуватися не пізніше, ніж через 12 місяців після опублікування цієї схеми, але не раніше дати, зазначеної на в пункті (c) частини 2 цієї статті.

4. Незважаючи на пункт (с) частини 2 цієї статті, держава-член може вирішити, що засоби електронної ідентифікації за схемою електронної ідентифікації, нотифікованої відповідно до частини 1 статті 9 іншою державою-членом, визнаються першою державою-членом з дати застосування виконавчих актів, про які йдеться в частині 2 статті 8 та частині 8 статті 12. Держави-члени, яких це стосується, повинні повідомити Комісію. Комісія оприлюднює зазначену інформацію.

Цей Регламент, повинен бути обов'язковим у повному обсязі та підлягає прямому застосуванню в усіх державах-членах.

Вчинено в Брюсселі 23 липня 2014 року

За Парламент

Голова

M. SCHULZ

За Раду

Голова

S. GOZI

*ДОДАТОК I***ВИМОГИ, ЩО ЗАСТОСОВУЮТЬСЯ ДО КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ЕЛЕКТРОННОГО ПІДПISУ**

Кваліфіковані сертифікати електронного підпису містять:

- (a) позначку, принаймні у формі, придатній для автоматизованої обробки, що сертифікат був виданий в якості кваліфікованого сертифіката електронного підпису;
 - (b) набір даних, які однозначно визначають кваліфікованого провайдера довірчих послуг, що видає кваліфіковані сертифікати, і містить, принаймні, назву держави-члена, на території якої було засновано цього провайдера, та:
 - для юридичної особи: назву та, в разі необхідності, реєстраційний номер, що міститься в офіційних реєстрах,
 - для фізичної особи: ім'я особи;
 - (c) принаймні, ім'я підписувача або псевдонім, якщо використовується псевдонім – це має бути чітко зазначено;
 - (d) дані перевірки на достовірність електронного підпису, які відповідають даним для створення електронного підпису;
 - (e) уточнення щодо початку та завершення строку дії сертифіката;
 - (f) ідентифікаційний код сертифікату, що має бути унікальним для кваліфікованого провайдера довірчих послуг;
 - (g) удосконалений електронний підпис або удосконалену електронну печатку кваліфікованого провайдера довірчих послуг, який видає сертифікат;
 - (h) місце, де можна безоплатно отримати сертифікат, на якому проставлено зазначені в пункті (g), удосконалений електронний підпис або удосконалену електронну печатку;
 - (i) місце надання послуги перевірки статусу чинності сертифіката, яка може бути використана для отримання інформації про статус чинності кваліфікованого сертифіката;
 - (j) якщо дані для створення електронного підпису, пов'язані з даними для перевірки достовірності електронного підпису знаходяться у засобах для створення кваліфікованого електронного підпису, повинна бути позначка про це, щонайменше в формі, придатній для автоматизованої обробки.
-

*ДОДАТОК II***ВИМОГИ, ЩО ЗАСТОСОВУЮТЬСЯ ДО КВАЛІФІКОВАНИХ ЗАСОБІВ ДЛЯ
СТВОРЕННЯ ЕЛЕКТРОННОГО ПІДПISУ**

1. Засоби для створення кваліфікованого електронного підпису забезпечують за допомогою належних технічних засобів та процедур, щонайменше:
 - (a) достатній рівень конфіденційності даних для створення електронного підпису, що використовуються для створення електронного підпису;
 - (b) що дані для створення електронного підпису, які використовуються для створення електронного підпису, практично визначаються лише один раз;
 - (c) наявність достатньої гарантії того, що дані для створення електронного підпису, які використовуються для створення електронного підпису, не можуть бути знайдені дедуктивним шляхом та, що електронний підпис має надійний захист від підробки шляхом використання наявних на даний час технічних засобів;
 - (d) надійний захист законним підписувачем від використання іншими особами даних для створення електронного підпису, що використовуються для створення електронного підпису.
 2. Кваліфіковані засоби для створення електронного підпису не змінюють дані, що підписуються, та не перешкоджають представленню таких даних підписувачу до підписання.
 3. Генерування та управління даними для створення електронного підпису від імені підписувача можуть здійснюватись виключно кваліфікованим провайдером довірчих послуг.
 4. Не порушуючи вимоги підпункту (d) частини 1, кваліфіковані провайдери довірчих послуг, що управляють даними для створення електронного підпису від імені підписувача, можуть відтворювати дані для створення електронного підпису лише в цілях захисту, за умови дотримання наступних вимог:
 - (a) рівень безпеки відтворених блоків даних повинен бути аналогічним рівню безпеки оригінальних блоків даних;
 - (b) кількість відтворених блоків даних не повинна перевищувати мінімальну кількість, необхідну для забезпечення безперервності обслуговування.
-

*ДОДАТОК III***ВИМОГИ, ЩО ЗАСТОСОВУЮТЬСЯ ДО КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ****ЕЛЕКТРОННИХ ПЕЧАТОК**

Кваліфіковані сертифікати електронної печатки містять:

- (a) позначку, принаймні у формі, придатній для автоматизованої обробки, що сертифікат був виданий в якості кваліфікованого сертифіката електронної печатки;
 - (b) набір даних, які однозначно визначають кваліфікованого провайдера довірчих послуг, що видає кваліфіковані сертифікати, і містить, принаймні, назву держави-члена, на території якої було засновано цього провайдера, та:
 - для юридичної особи: назву та, в разі необхідності, реєстраційний номер, що міститься в офіційних реєстрах,
 - для фізичної особи: ім'я особи;
 - (c) принаймні, ім'я розробника печатки та, в разі необхідності, реєстраційний номер, що міститься в офіційних реєстрах;
 - (d) дані перевірки на достовірність електронної печатки, які відповідають даним для створення електронної печатки;
 - (e) уточнення щодо початку та завершення строку дії сертифіката;
 - (f) ідентифікаційний код сертифікату, що має бути унікальним для кваліфікованого провайдера довірчих послуг;
 - (g) удосконалений електронний підпис або удосконалену електронну печатку кваліфікованого провайдера довірчих послуг, який видає сертифікат;
 - (h) місце, де можна безоплатно отримати сертифікат, на якому проставлено зазначені в пункті (g), удосконалений електронний підпис або удосконалену електронну печатку;
 - (i) місце надання послуги перевірки статусу чинності сертифіката, яка може бути використана для отримання інформації про статус чинності кваліфікованого сертифіката;
 - (j) якщо дані для створення електронної печатки, пов'язані з даними для перевірки достовірності електронної печатки знаходяться у засобах для створення кваліфікованої електронної печатки, повинна бути позначка про це, щонайменше в формі, придатній для автоматизованої обробки.
-

*ДОДАТОК IV***ВИМОГИ, ЩО ЗАСТОСОВУЮТЬСЯ ДО КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ****АВТЕНТИФІКАЦІЯ ВЕБ-САЙТУ**

Кваліфіковані сертифікати автентифікації веб-сайту повинні містити:

- (a) позначку, принаймні у формі, придатній для автоматизованої обробки, що сертифікат був виданий в якості кваліфікованого сертифіката автентифікації веб-сайту;
- (b) набір даних, які однозначно визначають кваліфікованого провайдера довірчих послуг, що видає кваліфіковані сертифікати, і містить, принаймні, назву держави-члена, на території якої було засновано цього провайдера, та:
 - для юридичної особи: назву та, в разі необхідності, реєстраційний номер, що міститься в офіційних реєстрах,
 - для фізичної особи: ім'я особи;
- (c) для фізичних осіб: принаймні, ім'я або псевдонім особи, якій був виданий сертифікат. Якщо використовується псевдонім, це повинно бути чітко зазначено;
 - для юридичних осіб: принаймні, назву юридичної особи, якій видано сертифікат, та, в разі необхідності, її реєстраційний номер, що міститься в офіційних реєстрах;
- (d) елементи адреси, серед яких, щонайменше, місто та Держава, фізичної або юридичної особи, якій було видано сертифікат та, в разі необхідності, зазначені елементи в тому вигляді, в якому вони містяться в офіційних реєстрах;
- (e) назву (назви) домену, який використовує фізична або юридична особа, якій видано сертифікат;
- (f) уточнення щодо початку та завершення строку дії сертифіката;
- (g) ідентифікаційний код сертифікату, що має бути унікальним для кваліфікованого провайдера довірчих послуг;
- (h) удосконалений електронний підпис або удосконалену електронну печатку кваліфікованого провайдера довірчих послуг, який видає сертифікат;
- (i) місце, де можна безоплатно отримати сертифікат, на якому проставлено зазначені в пункті (g), удосконалений електронний підпис або удосконалену електронну печатку;
- (j) місце надання послуги перевірки статусу чинності сертифіката, яка може бути використана для отримання інформації про статус чинності кваліфікованого сертифіката;