

Пропозиція стосовно Регламенту Європейського Парламенту і Ради щодо внесення змін до Регламенту (ЄС) № 910/2014 про встановлення системи європейської цифрової ідентичності

Пояснювальна записка

1. Зміст пропозиції

• Причини та цілі пропозиції

Ця пояснювальна записка супроводжує пропозицію щодо Регламенту Європейського Парламенту та Ради стосовно внесення змін до Регламенту (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та електронних довірчих послуг для електронних транзакцій на внутрішньому ринку (Регламент).

Документ має на меті забезпечити для транскордонного використання:

- доступ до високо безпечних та надійних рішень для цифрової ідентичності,
- що публічні та приватні послуги можуть покладатися на надійні та безпечні рішення для цифрової ідентичності,
- що фізичні та юридичні особи мають право використовувати рішення для цифрової ідентичності,
- що ці рішення пов'язані з різноманітними документами і дозволяють цілеспрямований обмін даними, що ідентифікують особу, з встановленням обмежень задля надання конкретної послуги,
- прийняття кваліфікованих електронних довірчих послуг у ЄС та рівних умов їх надання.

Те, що з'являється на ринку - це нове середовище, де фокус змістився від надання та використання жорсткої цифрової ідентичності до надання та залежність від конкретних документів, пов'язаних з цифровою ідентичністю. Зростає попит на рішення для забезпечення цифрової ідентичності, які можуть гарантувати ці можливості, забезпечуючи підвищення ефективності та високий рівень довіри в ЄС, як у приватному, так і в публічному секторі, спираючись на необхідність ідентифікувати та автентифікувати користувачів, забезпечуючи при цьому високий рівень надійності.

Оцінка нового Регламенту про встановлення основ для європейської цифрової ідентичності показала, що чинний Регламент не відповідає новим вимогам ринку, здебільшого через властиві йому обмеження для публічного сектора, обмежені можливості та складність підключення приватних провайдерів до системи, його недостатню кількість цифрових рішень щодо електронної ідентифікації у всіх державах-членах та відсутність гнучкості для підтримки різноманітних випадків використання. Крім того, рішення щодо цифрової ідентичності, що виходять за межі сфери застосування Регламенту, наприклад, запропоновані провайдерами соціальних медіа та фінансовими установами, викликають занепокоєння щодо конфіденційності та захисту даних. Вони не можуть ефективно реагувати на нові вимоги ринку та не мають транскордонного охоплення для вирішення конкретних галузевих потреб, де ідентифікація є чутливою та вимагає високого ступеня визначеності.

З моменту набрання чинності частини Регламенту присвяченого електронній ідентифікації у вересні 2018 року лише 14 держав-членів повідомили принаймні про одну схему електронної ідентифікації. Як наслідок, лише 59 % осіб, які проживають у ЄС мають доступ до надійних та безпечних транскордонних схем електронної ідентифікації. Лише 7 схем повністю мобільні, відповідаючи при цьому поточним очікуванням користувачів. Оскільки не всі технічні вузли забезпечують інтероперабельність відповідно до положень Регламенту (eIDAS) та є повністю функціональними, транскордонний доступ обмежений; Регламент забезпечує можливість отримати транскордонний доступ до небагатьох державних онлайн-послуг, доступних всередині країни.

Пропонуючи європейську систему цифрової ідентичності на основі перегляду поточної, щонайменше 80% громадян повинні мати можливість використовувати рішення для цифрової ідентифікації для доступу до ключових державних послуг до 2030 року. Система цифрової ідентичності повинна дати громадянам та особам, що проживають в ЄС повну впевненість у тому, що Європейська система цифрової ідентичності запропонує кожному можливість контролювати, хто має доступ до їхнього цифрового близнюка та до яких даних саме. Це також вимагатиме високого рівня безпеки щодо всіх аспектів надання цифрової ідентичності, включаючи видачу Європейського гаманця з цифровою ідентичністю, а також інфраструктури для збору, зберігання та розкриття даних, що ідентифікують особу

Крім того, нинішня система відповідно до Регламенту eIDAS (електронної ідентифікації, автентифікації та електронних довірчих послуг відповідно) не охоплює надання електронних документів, таких як медичні сертифікати або професійна кваліфікація, що ускладнює забезпечення загальноєвропейського юридичного визнання таких облікових даних в електронній формі. Крім того, Регламент eIDAS не дозволяє користувачам обмежувати спільний доступ до ідентифікаційних даних тим, що необхідно для надання послуги.

Хоча оцінка Регламенту eIDAS показує, що система надання електронних довірчих послуг була досить успішною, забезпечуючи високий рівень довіри та гарантуючи впровадження та використання більшості електронних довірчих послуг, для досягнення повної гармонізації та прийняття необхідно зробити ще більше. Для отримання кваліфікованих сертифікатів автентифікації веб-сайту громадяни повинні мати можливість покладатися на них і користуватися безпечною та надійною інформацією про те, хто стоїть за веб-сайтом, що зменшує ризик шахрайства.

Крім того, щоб реагувати на динаміку розвитку ринків та технологічний розвиток, ця Пропозиція розширює поточний перелік електронних довірчих послуг, передбачений Регламентом eIDAS трьома новими кваліфікованими довірчими послугами, а саме надання послуг електронного архівування, електронних книг обліку та управління віддаленим електронним підписом та пристрої для створення печаток.

Новий Регламент також пропонує гармонізований підхід до безпеки для громадян, які покладаються на європейську цифрову ідентичність, що представляє їх в мережі Інтернет, та для постачальників онлайн-послуг, які зможуть повністю покладатися на рішення цифрової ідентичності та приймати їх незалежно від того, де вони були видані. Ця Пропозиція передбачає зміну для емітентів європейських рішень у сфері цифрової ідентичності, забезпечуючи спільну технічну архітектуру та довідкову базу та загальні стандарти, які будуть розроблятися у співпраці з державами-членами. Необхідний

гармонізований підхід, щоб уникнути того, що розробка нових рішень щодо цифрової ідентичності в державах-членах створить подальшу фрагментацію, спричинену використанням різних національних рішень. Гармонізований підхід також зміцнить єдиний ринок, оскільки дозволить громадянам, іншим мешканцям та підприємствам здійснювати ідентифікацію в Інтернеті безпечним, зручним та єдиним способом у межах ЄС для доступу, як до послуг у публічних, так і до приватних послуг. Користувачі зможуть покладатися на вдосконалену екосистему для електронної ідентичності та довіри, які визнаються та приймаються в усіх державах-членах ЄС.

Щоб уникнути фрагментації та бар'єрів через різні стандарти, Комісія прийме Рекомендацію одночасно з цією пропозицією. Ця Рекомендація визначатиме процес підтримки спільного підходу, що дозволяє державам-членам та іншим зацікавленим сторонам із державного та приватного секторів у тісній координації з Комісією працювати над розробкою набору інструментів, щоб уникнути розбіжностей у підходах та уникнути загрози для майбутнього впровадження Європейської системи цифрової ідентичності.

Відповідність існуючим положенням у сфері цифрової ідентичності

Ця Пропозиція базується на чинному Регламенті eIDAS, на ролі держав-членів як тих, хто забезпечує правову ідентичність та на основі надання електронних довірчих послуг у Європейському Союзі. Пропозиція доповнює та повністю узгоджується з іншими інструментами політики стосовно цифрової ідентичності на рівні ЄС, що спрямовані на використання переваг внутрішнього ринку в цифровому світі, зокрема шляхом збільшення можливостей громадян отримувати доступ до транскордонних послуг. У цьому відношенні пропозиція реалізує політичний мандат, наданий Європейською Радою та Головою Європейської Комісії, щоб створити загальноєвропейську систему для цифрової ідентичності щодо надання публічних послуг, які гарантують, що будь-який громадянин чи резидент можуть мати доступ до безпечної ідентифікації, яка може бути використана в будь-якій точці ЄС для ідентифікації та автентифікації доступу до послуг у державному та приватному секторах, що дозволяє громадянам контролювати, які дані передаються та як вони використовуються.

Узгодженість з іншими політиками Союзу

Пропозиція узгоджується з пріоритетами цифрової трансформації, визначеними у стратегії «Формування цифрового майбутнього Європи», і підтримуватиме досягнення цілей, зазначених у Повідомленні про цифрове десятиліття. Будь-яка обробка персональних даних згідно з цим Регламентом повинна здійснюватися у повній відповідності до Загального регламенту захисту даних (надалі - GDPR). Крім того, цей Регламент запроваджує спеціальні гарантії захисту даних.

Для гарантування високого рівня безпеки ця пропозиція також узгоджується з політикою Союзу, що стосується кібербезпеки. Пропозиція була розроблена для зменшення фрагментації із застосуванням загальних вимог до кібербезпеки до постачальників електронних довірчих послуг, що регулюються Регламентом eIDAS.

Ця пропозиція, крім того, узгоджується з іншою секторальною політикою, що спирається на використання електронної ідентифікації, електронної атестації документів та інших електронних довірчих послуг. Це включає Положення про Єдиний цифровий шлюз, вимоги, які мають бути виконані у фінансовому секторі, пов'язані з боротьбою з відмиванням грошей та фінансуванням тероризму, ініціативи щодо спільного

використання облікових даних соціального страхування, для отримання посвідчення водія в цифровому форматі або для майбутніх цифрових проїзних документів та інші ініціативи, які мають зменшити адміністративний тягар для громадян та бізнесу, повністю покладаючись на можливості цифровізації процедур як у державному, так і в приватному секторі. Крім того, європейський гаманець з цифровою ідентичністю дозволить отримувати кваліфіковані електронні підписи, які можуть сприяти участі в політиці.

ПРАВОВА ОСНОВА, СУБСИДІАРНІСТЬ І ПРОПОРЦІЙНІСТЬ

• Правові підстави

Ця ініціатива спрямована на підтримку перетворення Союзу на єдиний цифровий ринок. Зі зростаючим оцифруванням транскордонних державних та приватних послуг, які ґрунтуються на використанні рішень для цифрової ідентичності, існує ризик того, що в рамках чинної законодавчої бази громадяни продовжуватимуть стикатися з перешкодами і не матимуть можливості повною мірою використовувати онлайн-послуги безперешкодно по всьому ЄС та для збереження їх конфіденційності. Існує також ризик того, що недоліки чинної правової бази щодо електронних електронних довірчих послуг збільшать фрагментацію та зменшать довіру, якщо залишити це лише на регулюванням державам-членам. Таким чином, стаття 114 ДФЄС визначена відповідною правовою основою цієї ініціативи.

Субсидіарність

Громадяни та підприємства повинні мати можливість скористатися наявністю високобезпечних та надійних рішень для цифрових ідентичності, які можна використовувати в усіх державах-членах ЄС, а також мобільністю електронної атестації документів для ідентифікації. Останні технологічні досягнення, ринок та попит користувачів вимагають наявності більш зручних для користувачів транскордонних рішень, які дозволяють отримати доступ до онлайн послуг в усіх державах-членах ЄС, чого не може запропонувати Регламент eIDAS у його нинішній формі.

Користувачі також дедалі частіше звикають до глобальних доступних рішень, наприклад, приймаючи використання рішень єдиного входу, що надаються платформами соціальних медіа для доступу до онлайн послуг. Держави-члени не можуть самостійно відповідати на виклики, зважаючи на ринкову силу великих постачальників, що вимагає взаємодії та надійних електронних ідентифікаторів на рівні ЄС. Крім того, електронна атестація документів, видана та прийнята в одній державі-члені, такі як електронний медичний сертифікат, часто не є юридично визнаною та прийнятою в інших державах-членах. Це створює ризик того, що держави-члени продовжуватимуть розробляти роздроблені національні рішення, які не можуть використовуватися транскордонно.

Що стосується надання електронних довірчих послуг, хоча вони значною мірою регулюються та функціонують відповідно до поточної правової системи, національна практика також створює ризик збільшення фрагментації.

Втручання на рівні ЄС в кінцевому підсумку найкраще підходить для надання громадянам та підприємствам для здійснення транскордонної ідентифікації та обміну особистими документами та ідентифікаційними даними за допомогою надзвичайно безпечних та надійних рішень щодо забезпечення цифрової ідентичності відповідно до правил захисту

даних ЄС. Для цього потрібні надійні та безпечні інструменти електронної ідентифікації та нормативна база, що пов'язує їх з документами та повноваженнями на рівні ЄС. Лише втручання на рівні ЄС може встановити гармонізовані умови, які забезпечують контроль користувача та доступ до транскордонних онлайн послуг, а також система взаємодії, що полегшує використання онлайн-послуг у забезпеченні безпечних рішень для цифрової ідентичності, незалежно від того, де в ЄС вона надана послуга або де проживає громадянин. Як значною мірою відображено в огляді Регламенту eIDAS, малоімовірно, що зусилля на національному рівні були б однаково ефективними та дієвими.

Пропорційність

Ця ініціатива є пропорційною досягнутим цілям, забезпечуючи відповідний інструмент для встановлення інтероперабельної структури для створення екосистеми Європейської цифрової ідентичності на основі встановлення ідентичності державами-членами, та положення щодо надання кваліфікованих та некваліфікованих документів цифрової ідентичності. Вона забезпечує чіткий внесок у досягнення мети щодо вдосконалення єдиного цифрового ринку за допомогою більш гармонізованої правової бази. Гармонізовані європейські гарантії з цифровою ідентичністю, які будуть випущені державами-членами на основі загальних технічних стандартів, також забезпечують загальний підхід ЄС, що приносить переваги користувачам та сторонам, які покладаються на наявність безпечних транскордонних рішень для електронної ідентифікації. Ця ініціатива вирішує обмеження існуючої системи інтероперабельності електронної ідентифікації на основі взаємного визнання різноманітних національних схем електронної ідентифікації. Беручи до уваги поставлені цілі, ця ініціатива вважається достатньо пропорційною, а витрати, ймовірно, будуть співмірними з потенційною вигодою. Запропонований Регламент спричинить фінансові та адміністративні витрати, які повинні нести держави-члени як емітенти європейських гарантіїв з цифровою ідентичністю, електронні довірчі послуги та постачальники онлайн послуг. Однак ці витрати, ймовірно, були б переважені значними потенційними вигодами для громадян та користувачів, що впливають безпосередньо із збільшення транскордонного визнання та прийняття електронної ідентичності та послуг з видачі документів.

Витрати на створення та приведення у відповідність до нових стандартів для постачальників електронних довірчих послуг та постачальників онлайн послуг неможливо уникнути, якщо потрібно досягти мети зручності та доступності. Ініціатива має намір використати та розвинути інвестиції, які вже зробили держави-члени у свої національні схеми щодо забезпечення цифрової ідентичності. Крім того, додаткові витрати, встановлені Пропозицією, розроблені для підтримки гармонізації правил та стандартів і обґрунтовані сподіванням, що в довгостроковій перспективі вони зменшать адміністративне навантаження та витрати на дотримання вимог. Витрати, пов'язані з прийняттям у регульованих секторах документів автентифікації цифрової ідентичності, також можна вважати необхідними та пропорційними, оскільки вони підтримують загальну мету та забезпечуються засобами, за допомогою яких регульовані сектори можуть виконувати юридичні зобов'язання щодо ідентифікації користувача.

Вибір інструменту

Вибір Регламенту як правового інструменту виправданий необхідністю забезпечення єдиних умов на внутрішньому ринку для застосування європейської цифрової ідентичності за допомогою гармонізованої бази, яка спрямована на створення безперебійної сумісності та забезпечення європейських громадян та компаній, які надають

публічні та приватні послуги по всьому Союзу надзвичайно безпечними та надійними електронними ідентифікаторами.

РЕЗУЛЬТАТИ ОЦІНЮВАННЯ, КОНСУЛЬТАЦІЙ ЗАЦІКАВЛЕНИХ СТОРІН ТА ОЦІНКА ВПЛИВУ

Оцінки/перевірки відповідності чинного законодавства

Оцінка функціонування Регламенту eIDAS була проведена в рамках процесу перегляду, передбаченого статтею 49 Регламенту eIDAS. Основні висновки оцінки щодо цифрової ідентичності полягають у тому, що eIDAS не досягла свого потенціалу. Було повідомлено, що лише обмежену кількість інструментів електронної ідентифікації було використано, що обмежує охоплення схем електронної ідентифікації приблизно 59% населення ЄС. Крім того, прийняття системи електронної ідентифікації як на рівні держав-членів, так і постачальниками послуг обмежене. Оціночне дослідження також виявило, що поточний обсяг та спрямованість Регламенту eIDAS на схеми електронної ідентифікації, про які повідомляють держави-члени ЄС, та на надання доступу до публічних онлайн послуг здаються занадто обмеженими та неадекватними. Переважна більшість потреб електронної ідентифікації та віддаленої автентифікації залишається у приватного сектору, зокрема в таких сферах, як банківські оператори, оператори зв'язку та платформи, які відповідно до законодавства зобов'язані перевіряти особу своїх клієнтів. Додана цінність Регламенту eIDAS щодо електронної ідентичності обмежена через його низьке охоплення, поширення та використання.

Проблеми, виявлені в цій пропозиції, пов'язані з недоліками поточної системи, передбаченої Регламентом eIDAS та фундаментальними змінами в контексті щодо ринків, суспільного та технологічного розвитку, що викликають потреби нових користувачів та ринку.

Консультації зацікавлених сторін

Відкрите громадське обговорення розпочалося 24 липня 2020 року та було завершено 2 жовтня 2020 року. Загалом Комісія отримала 318 пропозицій. Комісія також отримала 106 відповідей на цільове опитування зацікавлених сторін. Держави-члени також збирали думки на різних двосторонніх та багатосторонніх зустрічах та опитуваннях, організованих з початку 2020 року. Це зокрема включає опитування представників держав-членів Мережі співробітництва eIDAS у липні-серпні 2020 року та різні спеціальні семінари. Комісія також провела ґрунтовні інтерв'ю з представниками галузі та зустрілася із зацікавленими сторонами бізнесу у різних секторах (наприклад, електронна комерція, охорона здоров'я, фінансові послуги, оператори зв'язку, виробники обладнання тощо) на двосторонніх зустрічах.

Переважає більшість респондентів на відкритих публічних консультаціях привітали створення єдиної системи цифрової ідентичності в рамках ЄС, що спирається на систему електронної ідентифікації держав-членів ЄС. Держави-члени значною мірою підтримують необхідність посилення чинного Регламенту eIDAS, що надає громадянам можливість доступу як до публічних, так і до приватних послуг, і визнають необхідність створення електронної довірчої послуги, що дозволяє видавати та транскордонно використовувати послугу з електронної атестації документів. В цілому, держави-члени підкреслили необхідність побудови Європейської системи цифрової ідентичності на основі досвіду та

національних рішень, прагнучи знайти синергію та отримати вигоду від здійснених інвестицій. Багато зацікавлених сторін згадували, як пандемія COVID-19 продемонструвала цінність безпечної, віддаленої ідентифікації для доступу всіх до публічних та приватних послуг. Щодо електронних довірчих послуг, більшість суб'єктів погоджуються з тим, що нинішні рамки досягли успіху, проте були потрібні деякі додаткові заходи для подальшої гармонізації певної практики, пов'язаної з дистанційною ідентифікацією та національним наглядом. Зацікавлені сторони з переважно національною базою клієнтів висловили більше сумнівів щодо доданої вартості європейської системи цифрової ідентичності.

Гаманці з цифровою ідентичністю все більше сприймаються державним та приватним сектором як найбільш відповідний інструмент, що дозволяє користувачам вибирати, коли і з яким приватним постачальником послуг поділитися різними документами, залежно від варіанту використання та безпеки, необхідної для відповідної транзакції. Цифрова ідентифікація на основі цифрових гаманців, які надійно зберігаються на мобільних пристроях, були визначені як основний ресурс для перспективного рішення. І приватний ринок (наприклад, Apple, Google, Thales) та уряди вже рухаються в цьому напрямку.

Збір та використання експертизи

Пропозиція базується на інформації, зібраній у рамках консультацій із зацікавленими сторонами з метою оцінки впливу та звітів про оцінку Регламенту eIDAS з огляду на зобов'язання щодо перегляду, визначені у статті 49 Регламенту eIDAS. Було організовано численні зустрічі з представниками держав-членів та експертами.

Оцінка впливу

Для цієї пропозиції була проведена оцінка впливу. 19 березня 2021 року Комітет з регуляторного контролю видав негативний висновок з деякими коментарями. Після перегляду повторного подання 5 травня 2021 року Рада надала позитивний висновок.

Комісія вивчає різні варіанти політики для досягнення загальної мети цієї ініціативи, а саме забезпечення належного функціонування внутрішнього ринку, особливо стосовно надання та використання високобезпечних та надійних рішень електронної ідентифікації.

Оцінка впливу вивчає базовий сценарій, варіанти політики та їх вплив для трьох розглянутих варіантів політики. Кожен варіант пропонує вибір для політичного розгляду на основі рівня амбіцій. Перший варіант передбачає низький рівень амбіцій та комплекс заходів, головним чином спрямованих на підвищення ефективності та дієвості чинного Регламенту eIDAS. Вводячи обов'язкове повідомлення про національні електронні посвідчення та вдосконалюючи існуючі інструменти для досягнення взаємного визнання, перший варіант ґрунтується на задоволенні потреб громадян, спираючись на наявність різноманітних національних схем електронної ідентифікації, які мають на меті стати сумісними.

Другий варіант передбачає середній рівень амбіцій і, головним чином, спрямований на розширення можливостей безпечного обміну даними, пов'язаними з електронною ідентифікацією, доповнюючи національні електронні свідоцтва та підтримуючи поточний перехід до послуг з електронної ідентифікації. Метою цього варіанту було б задовольнити попит користувачів та створити нову кваліфіковану послугу – електронної атестації

документів, пов'язаних із надійними джерелами, та забезпечення транскордонного визнання. Це розширило б сферу застосування поточного Регламенту eIDAS та підтримало б якомога більше випадків використання, спираючись на необхідність перевірки документів електронної ідентифікації, пов'язаних з високим рівнем гарантій надійності.

Третій і бажаний варіант представляє найвищий рівень амбіцій та спрямований на регулювання положень щодо високо захищеного особистого цифрового гаманця з цифровою ідентичністю, виданого державами-членами. Цей варіант є найбільш бажаним варіантом для реалізації цілей цієї ініціативи. Для повного задоволення політичних цілей цей варіант спирається на більшість заходів, які оцінюються згідно з варіантом один (залежність від цифрової ідентичності, засвідченої державами-членами, та наявність взаємовизнаних засобів електронної ідентифікації) та другого варіанту (електронна атестація документів з транскордонним визнанням).

Що стосується загальної системи для електронних довірчих послуг, то рівень амбіційності вимагає набору заходів, які не потребують покрокового підходу для досягнення цілей політики.

Новий кваліфікований електронний довірчий сервіс для управління пристроями для віддаленого створення електронного підпису та печатки принесе значну безпеку, єдність, юридичну визначеність та переваги вибору споживача як у зв'язку з сертифікацією пристроїв створення кваліфікованих підписів, так і у зв'язку з вимогами, які повинні бути виконані кваліфіковані постачальники довірчих послуг, які керують такими пристроями. Нові положення зміцнять загальну нормативну базу та систему нагляду за наданням електронних довірчих послуг.

Вплив варіантів політики на різні категорії зацікавлених сторін детально пояснюється у Додатку 3 до Оцінки впливу, що підтримує цю ініціативу. Оцінка є кількісною та якісною. Дослідження оцінки впливу показує, що мінімальні кількісні витрати можна оцінити в 3,2+ мільярда євро, оскільки деякі статті витрат неможливо визначити кількісно. Загальні підраховані вигоди оцінюються в 3,9-9,6 млрд євро. Що стосується більш широких економічних наслідків, очікується, що бажаний варіант матиме позитивний вплив на інновації, міжнародну торгівлю та конкурентоспроможність, сприятиме економічному зростанню та призведе до додаткових інвестицій у рішення для цифрової ідентичності. Наприклад, очікується, що додаткові інвестиції в розмірі 500 мільйонів євро, викликані законодавчими змінами згідно з варіантом 3, принесуть вигоди у розмірі 1,268 мільйонів євро через 10 років (при прийнятті 67%).

Очікується, що бажаний варіант також матиме позитивний вплив на зайнятість, створивши від 5 000 до 27 000 додаткових робочих місць протягом 5 років після впровадження. Це пояснюється додатковими інвестиціями та зменшенням витрат для підприємств, які покладаються на використання рішень електронної ідентифікації.

Очікується, що позитивний вплив на навколишнє середовище буде найбільшим для третього варіанту, який, як очікується, максимально покращить поглинання та використання електронної ідентифікації, надавши позитивний вплив на скорочення викидів, пов'язаних з наданням публічних послуг.

Електронні облікові книги надають користувачам докази та незмінний аудиторський слід для послідовності транзакцій та записів даних, гарантуючи цілісність даних. Хоча ця

електронна довірча послуга не була частиною оцінки впливу, вона ґрунтується на існуючих електронних довірчих сервісах, оскільки поєднує в собі позначення часу та їх послідовність із певністю щодо джерела даних, що є подібним до електронного підпису. Ця електронна довірча послуга необхідна для запобігання фрагментації внутрішнього ринку шляхом визначення єдиної загальноєвропейської системи, яка дозволяє транскордонне визнання електронних довірчих послуг, що підтримують роботу кваліфікованих електронних облікових книг. Цілісність даних, у свою чергу, дуже важлива для об'єднання даних з децентралізованих джерел, для самостійних рішень з електронної ідентифікації, для запису права власності на цифрові активи, для запису бізнес-процесів для перевірки відповідності критеріям сталості та для різних випадків використання на ринках капіталу

Нормативне регулювання та спрощення

Ця пропозиція визначає заходи, які будуть застосовуватися до органів державної влади, громадян та постачальників онлайн послуг. Це зменшить адміністративні витрати та витрати щодо відповідності положенням Регламенту для державних адміністрацій та операційні витрати, а також скоротить витрати, пов'язані з безпекою, для постачальників онлайн послуг. Громадяни виграють на економії від зменшення адміністративного навантаження, повністю покладаючись на цифрові засоби ідентифікації та можливість безпечного обміну документами з однаковим юридичним транскордонним визнанням. Постачальники електронних ідентифікаційних даних також виграють від економії витрат на відповідність вимогам.

Основні права

Оскільки персональні дані підпадають під сферу застосування деяких елементів Регламенту, заходи розроблені таким чином, щоб повністю відповідати законодавству про захист даних. Наприклад, пропозиція покращує варіанти обміну даними та дає можливість дискреційного розкриття інформації. За допомогою європейського гаманця з цифровою ідентифікацією користувач зможе контролювати, яка кількість даних надається належним сторонам, та бути поінформованим про документи, необхідні для надання певної послуги. Постачальники послуг інформують держав-членів про свій намір спиратися на європейські гаманці з цифровою ідентичністю, що дозволить державам-членам контролювати те, що набори конфіденційних даних, наприклад, що стосуються здоров'я, запитуються лише постачальниками послуг відповідно до національного законодавства.

БЮДЖЕТНИЙ ВПЛИВ

Для оптимального досягнення цілей цієї ініціативи необхідно фінансувати низку заходів як на рівні Комісії, де передбачається виділення близько 60 ЕПВ протягом 2022-2027 років, так і на рівні держав-членів шляхом їх активної участі в експертних групах та комітетах, пов'язаних з роботою ініціативи, до складу яких входять представники держав-членів. Загальні фінансові ресурси, необхідні для реалізації пропозиції у період 2022-2027 років, становитимуть до 30,825 млн євро, у тому числі 8,825 млн євро адміністративних витрат та до 22 млн євро операційних витрат, передбачених Програмою «Цифрова Європа» (очікується угода). Фінансування підтримуватиме витрати, пов'язані з підтримкою, розробкою, розміщенням, експлуатацією та підтримкою есистеми електронної ідентифікації та системи побудови електронних довірчих послуг. Він також може підтримувати гранти на підключення послуг до екосистеми європейського гаманця з цифровою ідентичністю, розробку стандартів та технічних специфікацій. Нарешті,

фінансування також сприятиме проведенню щорічних опитувань та досліджень і ефективності регулювання у досягненні його цілей. "Фінансова звітність", пов'язана з цією ініціативою, містить детальний огляд витрат.

- Плани впровадження та механізми моніторингу, оцінки та звітності

Вплив буде моніторитися та оцінюватись відповідно до Керівних принципів кращого регулювання, що охоплюють впровадження та застосування запропонованого Регламенту. Домовленість про моніторинг становить важливу частину пропозиції, зокрема з огляду на недоліки поточної системи звітності, як показано в оціночному дослідженні. Окрім вимог до звітності, запроваджених у запропонованому Регламенті, які мають на меті забезпечити кращу базу даних та аналізу, рамки моніторингу охоплюватимуть: 1) наскільки необхідні зміни були впроваджені відповідно до прийнятих заходів; 2) чи були впроваджені необхідні зміни до відповідних національних систем; 3) чи були дотримані необхідні зміни до зобов'язань щодо дотримання вимог відповідними суб'єктами. Європейська Комісія (1, 2 і 3) та національні компетентні органи (2 і 3) будуть відповідати за збір даних на основі заздалегідь визначених показників.

Щодо застосування запропонованого інструменту, Європейська Комісія та національні компетентні органи оцінюватимуть за допомогою щорічних опитувань: 1) доступ до засобів електронної ідентифікації для всіх громадян ЄС; 2) посилення транскордонного визнання та прийняття схем електронної ідентифікації; 3) заходи щодо стимулювання прийняття приватним сектором та розвитку нових послуг цифрової ідентичності.

Європейська Комісія збиратиме контекстну інформацію, використовуючи щорічні опитування щодо: 1) розміру ринку електронної ідентифікації; 2) витрати на державні закупівлі, пов'язані з електронною ідентифікацією; 3) частка підприємств, що надають свої послуги в Інтернеті; 4) частка онлайн-транзакцій, що вимагають чіткої ідентифікації клієнта; 5) частка громадян ЄС, які користуються онлайн приватними та державними послугами.

Детальне пояснення конкретних положень пропозиції

Проект Регламенту вимагає від держав-членів у статті 6a видавати Європейський гаманець з цифровою ідентичністю відповідно до схваленої схеми електронної ідентифікації відповідно до загальних технічних стандартів після обов'язкової оцінки відповідності та добровільної сертифікації в рамках європейської системи сертифікації кібербезпеки, як це встановлено Законом про кібербезпеку. Він включає положення, які забезпечують можливість фізичних та юридичних осіб мати можливість безпечно запитувати та отримувати, зберігати, поєднувати та використовувати ідентифікаційні дані осіб та електронну атестацію документів для автентифікації в Інтернеті та офлайн, а також дозволяти доступ до товарів та онлайн державних та приватних послуг під контролем користувача. Ця сертифікація не завдає шкоди GDPR у тому сенсі, що операції з обробки персональних даних, пов'язані з європейським гаманцем з цифровою ідентичністю, можуть бути сертифіковані лише відповідно до статей 42 та 43 GDPR.

Пропозиція встановлює у статті 6b конкретні положення щодо вимог, що застосовуються до належних сторін щодо запобігання шахрайству та забезпечення автентифікації особистих ідентифікаційних даних та електронної тестастії документів, що походять з європейського гаманця з цифровою ідентичністю.

З метою розширення доступності засобів електронної ідентифікації для транскордонного використання та підвищення ефективності процесу взаємного визнання повідомлених схем електронної ідентифікації, повідомлення про принаймні одну схему електронної ідентифікації державами-членами є обов'язковим у статті 7. Крім того, додано положення, що сприяють унікальній ідентифікації для забезпечення унікальної та постійної ідентифікації фізичних осіб у статті 11а. Це стосується випадків, коли законодавство вимагає ідентифікації, наприклад, у сфері охорони здоров'я, у сфері фінансів для виконання зобов'язань щодо боротьби з відмиванням грошей або для судового розгляду. З цією метою держави-члени повинні будуть включити унікальний та постійний ідентифікатор до мінімального набору даних для ідентифікації осіб. Можливість держав-членів спиратися на сертифікацію для забезпечення відповідності Регламенту і тим самим замінюючи процес експертної перевірки, покращує ефективність взаємного визнання.

У розділі 3 представлені нові положення щодо транскордонної залежності від європейського гаманця з цифровою ідентичністю, щоб гарантувати, що користувачі можуть покладатися на використання європейських гаманців з цифровою ідентичністю для доступу до онлайн послуг, що надаються органами державної влади та приватними постачальниками послуг, які потребують використання потужних систем автентифікації користувача.

У розділі III про електронні довірчі послуги до статті 14 про міжнародні аспекти вносяться зміни, щоб дозволити Комісії ухвалювати імплементаційні рішення, що засвідчують еквівалентність вимог, що застосовуються до електронних довірчих послуг, встановлених у третіх країнах, та послуг, які вони надають, на додаток до використання угод про взаємне визнання відповідно до статті 218 ДФЕС.

Щодо загальних положень, що застосовуються до довірчих послуг, включаючи кваліфікованих постачальників довірчих послуг, до статей 17, 18, 20, 21 та 24 вносяться зміни з метою узгодження з правилами, що застосовуються до безпеки мережі та інформації в ЄС. Що стосується методів, які мають використовувати кваліфіковані постачальники електронних довірчих послуг для перевірки ідентичності фізичних чи юридичних осіб, яким видаються кваліфіковані сертифікати, положення про використання дистанційних засобів ідентифікації були гармонізовані та уточнені з метою забезпечити, щоб однакові правила застосовувалися в усьому ЄС.

У главі III представлена нова стаття 29а, що визначає вимоги до кваліфікованої послуги управління віддаленими пристроями створення електронного підпису. Нова кваліфікована довірна послуга буде безпосередньо пов'язана і будуватиметься на заходах, на які посилаються та оцінюються в оцінці впливу, зокрема на заходи щодо "Гармонізації процесу сертифікації віддаленого електронного підпису" та інші заходи, що вимагають гармонізації наглядової практики державами-членами.

Для того, щоб користувачі могли ідентифікувати, хто стоїть за веб-сайтом, до статті 45 вносяться зміни, які вимагають від постачальників веб-браузерів полегшити використання кваліфікованих сертифікатів для автентифікації веб-сайту.

У розділі III представлено три нові частини.

Новий розділ 9 містить положення про правові наслідки електронної атестації документів, їх використання у визначених секторах та вимоги до кваліфікованої електронної атестації

документів. З метою забезпечення високого рівня довіри до статті 45d додається положення про перевірку документів щодо достовірності джерел. Щоб переконатися, що користувачі європейського гаманця з цифровою ідентичністю можуть скористатися наявністю електронних атестатів документів і мати такі атестати, видані у відповідності до послуги європейському гаманця з цифровою ідентичністю, у статтю 45e додається вимога. Натомість у статті 45f містяться додаткові правила надання електронної атестації документів, у тому числі щодо захисту персональних даних.

Новий розділ 10 передбачає надання кваліфікованих послуг електронного архівування на рівні ЄС. Стаття 45g про кваліфіковані послуги електронного архівування доповнює статті 34 та 40 про кваліфіковані послуги зі збереження кваліфікованих електронних підписів та кваліфікованих електронних печаток.

Новий розділ 11 встановлює рамки для електронних довірчих послуг щодо створення та обслуговування електронних облікових книг та кваліфікованих електронних облікових книг. Електронна облікова книга поєднує в собі відмітку часу та їх послідовність з упевненістю щодо особи, яка вносить дані, подібного до електронного підпису, з додатковою перевагою, що забезпечує більш децентралізоване управління, придатне для багатосторонньої співпраці. Це важливо для різних варіантів використання, які можуть бути побудовані на електронних облікових книгах.

Електронні облікові книги допомагають компаніям заощаджувати витрати, роблячи багатосторонню координацію більш ефективною, безпечною та полегшують регуляторний нагляд. За відсутності європейського регулювання існує ризик, що національні законодавці встановлять різні національні стандарти. Для запобігання фрагментації необхідно визначити єдину загальноєвропейську систему, яка дасть можливість трансграничного визнання електронних довірчих послуг, що підтримують функціонування електронних облікових книг. Цей загальноєвропейський стандарт для операторів вузлів застосовуватиметься, незважаючи на інше вторинне законодавство ЄС. Якщо електронні облікові книги використовуються для підтримки випуску та/або торгівлі облігаціями або для крипто-активів, варіанти використання повинні бути сумісними з усіма застосовними фінансовими правилами, наприклад, з Директивою про ринки фінансових інструментів, Директивою про платіжні послуги та майбутнім Положенням про ринки крипто-активів. Якщо випадки використання стосуються персональних даних, постачальникам послуг потрібно буде дотримуватися ЗРЗД.

75% усіх випадків використання електронних облікових книг були у банківському секторі та фінансовому секторі ще у 2017 році. Використання електронних облікових книг сьогодні стає все більш різноманітним, 17% - у сфері комунікацій та ЗМІ; 15% у виробництві та природних ресурсах, 10% у державному секторі, 8% у страхуванні, 5% у роздрібній торгівлі, 6% у транспорті, 5% у комунальних послугах.

Нарешті, глава VI містить нову статтю 48b, яка забезпечує збір статистичних даних щодо використання європейського гаманця з цифровою ідентичністю для моніторингу ефективності зміненого Регламенту 2021/0136 (COD)

Пропозиція РЕГЛАМЕНТУ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ щодо внесення змін до Регламенту (ЄС) No 910/2014 щодо встановлення системи європейської цифрової ідентичності

ЄВРОПЕЙСЬКИЙ ПАРЛАМЕНТ І РАДА ЄВРОПЕЙСЬКОГО СОЮЗУ,

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

Беручи до уваги пропозицію Європейської Комісії,

Після передачі проекту законодавчого акта національним парламентам,

Беручи до уваги висновок Європейського економічного та соціального комітету,

Діючи відповідно до звичайної законодавчої процедури,

Враховуючи:

(1) У Повідомленні Комісії від 19 лютого 2020 р. Під назвою “Формування цифрового майбутнього Європи” оголошується перегляд Регламенту (ЄС) No 910/2014 Європейського Парламенту та Ради з метою підвищення його ефективності та поширення його переваг на приватний сектор та встановити надійну систему цифрової ідентичності для всіх європейців.

(2) У своїх висновках від 1-2 жовтня 2020 р. Європейська Рада закликала Комісію запропонувати та розробити загальноєвропейський систему для безпечної публічної електронної ідентичності, включаючи сумісні цифрові підписи, щоб забезпечити людям контроль над їх онлайн ідентичністю та даними, а також дозволити доступ до державних, приватних та трансграничних цифрових послуг.

(3) У Повідомленні Комісії від 9 березня 2021 р. Під назвою «Цифровий компас до 2030 р.: Європейський шлях цифрового десятиліття» встановлено мету Союзу, яка до 2030 р. призведе до широкого впровадження безпечної системи електронної ідентичності, дозволяючи кожному користувачеві контролювати власні операції та присутність у мережі Інтернет.

(4) Більш гармонізований підхід до електронної ідентифікації повинен зменшити ризики та витрати поточної фрагментації через використання різних національних рішень та зміцнить єдиний ринок, дозволяючи громадянам, іншим резидентам, визначеним національним законодавством, та підприємствам проводити ідентифікацію в Інтернеті зручним та єдиним способом по всьому Союзу. Кожен повинен мати можливість безпечно отримувати доступ до державних та приватних послуг, спираючись на вдосконалену екосистему електронних довірчих послуг, а також на перевірені докази ідентичності та підтвердження документів, таких як університетський диплом, юридично визнаний та прийнятий скрізь у Союзі. Структура європейської цифрової ідентичності має на меті перехід від залежності лише від національних рішень щодо цифрової ідентичності до надання електронних атестатів документів, чинних на європейському рівні. Постачальники електронних атестатів документів повинні користуватися чітким та єдиним набором правил, а державні адміністрації повинні мати можливість покладатися на електронні документи у певному форматі.

(5) Для підтримки конкурентоспроможності європейського бізнесу постачальники онлайн послуг повинні мати можливість покладатися на рішення щодо цифрової ідентичності, визнані в усьому Союзі, незалежно від держави-члена, в якій вони були видані, таким чином отримуючи вигоду від гармонізованого європейського підходу до довіри, безпеки та

сумісності. Користувачі та постачальники послуг повинні мати можливість користуватися однаковим юридичним визнанням, що надається електронною атестацією документів по всьому Союзу.

(6) Регламент (ЄС) No 2016/679 застосовується до обробки персональних даних під час виконання цього Регламенту. Отже, цей Регламент повинен встановлювати спеціальні запобіжні заходи для запобігання тому, щоб постачальники засобів електронної ідентифікації та електронної атестації документів збирали персональні дані від інших послуг пов'язаних з необхідністю збирання персональних даних, що стосуються послуг, які підпадають під дію цього Регламенту.

(7) Необхідно встановити гармонізовані умови для створення системи для європейських гаманців з цифровою ідентичністю, які будуть видаватися державами-членами, що повинно надати всім громадянам Союзу та іншим резидентам, як це визначено національним законодавством, можливість гарантувати безпечний обмін даними, що стосуються їх ідентичності у зручному для користувача форматі під виключним контролем користувача. Технології, що використовуються для досягнення цих цілей, слід розвивати з метою досягнення найвищого рівня безпеки, зручності користувача та широкого використання. Держави-члени повинні забезпечити рівний доступ до електронної ідентифікації для всіх своїх громадян та резидентів.

(8) Для того, щоб забезпечити відповідність законодавству Союзу чи національному законодавству держава-членів Союзу, постачальники послуг повинні повідомити державам-членам про свій намір використовувати європейські гаманці цифрової ідентичності. Це дозволить державам-членам захищати користувачів від шахрайства та запобігати незаконному використанню даних, що посвідчують особу, та електронної атестації документів, а також гарантуватиме, що обробка конфіденційних даних, таких як дані про стан здоров'я, може бути перевірена належними сторонами відповідно до законодавства Союзу або національного законодавства.

(9) Усі Європейські гаманці з цифровою ідентичністю мають дозволяти користувачам забезпечувати транскордонну електронну ідентифікацію та автентифікацією в Інтернеті та офлайн для доступу до широкого кола державних та приватних послуг. Без шкоди для прерогатив держав-членів щодо ідентифікації їх громадян та резидентів, гаманці також можуть обслуговувати інституційні потреби державних адміністрацій, міжнародних організацій та установ, органів та установ Союзу. Використання офлайн було б важливим у багатьох секторах, включаючи сектор охорони здоров'я, де послуги часто надаються за допомогою особистої взаємодії, а електронні рецепти повинні мати можливість спиратися на QR-коди або подібні технології для перевірки справжності. Спираючись на «високий» рівень гарантії, Європейські гаманці з цифровою ідентичністю повинні користуватися інструментами, які пропонують рішення, що захищають від підробок, такі як захисні елементи, для дотримання вимог безпеки згідно з цим Регламентом. Європейські гаманці з цифровою ідентичністю також повинні дозволяти користувачам створювати та використовувати кваліфіковані електронні підписи та печатки, які прийняті в ЄС. Для досягнення спрощення та зменшення витрат для осіб та підприємств у ЄС, у тому числі шляхом надання повноважень представництва та електронних мандатів, держави-члени повинні видавати європейські гаманці цифрової ідентичності, спираючись на загальні стандарти, щоб забезпечити сумісність та високий рівень безпеки. Тільки компетентні органи держав-членів можуть забезпечити високий ступінь довіри у встановленні ідентичності особи, а отже, гарантувати, що особа, яка заявляє або підтверджує певну особу, насправді є тією особою, якою вона себе видає. Тому необхідно, щоб Європейські гаманці з цифровою ідентичністю здійснювали ідентифікацію громадян, інших резидентів

чи юридичних осіб. Довіра до європейських гаманців з цифровою ідентичністю буде посилена тим фактом, що сторони-емітенти зобов'язані впроваджувати відповідні технічні та організаційні заходи для забезпечення рівня безпеки, відповідного ризикам, що виникають для прав і свобод фізичних осіб, відповідно до Регламенту (ЄС) 2016/679.

(10) Для досягнення високого рівня безпеки та надійності цей Регламент встановлює вимоги до європейських гаманців з цифровою ідентичністю. Відповідність європейських гаманців з цифровою ідентичністю цим вимогам повинні бути сертифіковані акредитованими органами державного чи приватного сектору, відповідними державами-членами. Спираючись на схему сертифікації, що ґрунтується на наявності загальноприйнятих стандартів, державам-членам слід забезпечити високий рівень довіри та сумісності. Сертифікація, зокрема, повинна спиратися на відповідні європейські схеми сертифікації кібербезпеки, встановлені відповідно до Регламенту (ЄС) 2019/881. Така сертифікація не повинна завдавати шкоди сертифікації щодо обробки персональних даних відповідно до Регламенту (ЄС) 2016/679

(11) Європейські гаманці з цифровою ідентичністю повинні забезпечувати найвищий рівень безпеки персональних даних, що використовуються для автентифікації, незалежно від того, зберігаються ці дані локально або у хмарних сховищах, беручи до уваги різні рівні ризику. Використання біометрії для автентифікації є одним із методів ідентифікації, що забезпечує високий рівень впевненості, зокрема, коли використовується в поєднанні з іншими елементами автентифікації. Оскільки біометрія являє собою унікальну характеристику людини, використання біометрії вимагає організаційних та заходів безпеки, пропорційних ризику, що така обробка може спричинити за собою порушення прав та свобод фізичних осіб відповідно до Регламенту 2016/679.

(12) Щоб гарантувати, що Європейська система цифрової ідентичності відкрита для інновацій, технологічного розвитку та надійності майбутнього, держави-члени слід заохочувати до спільного створення платформ для тестування інноваційних рішень у контрольованому та безпечному середовищі, зокрема для покращення їх функціональності, захист персональних даних, безпеку та сумісність рішень та інформування про майбутні оновлення технічних посилань та законодавчих вимог. Таке середовище має сприяти приєднанню європейських малих та середніх підприємств, стартапів та окремих розробників інновацій і дослідників.

(13) Регламент (ЄС) No 2019/1157 посилює безпеку ідентифікаційних карток з розширеними функціями безпеки до серпня 2021 р. Державам-членам слід розглянути можливість їх повідомлення в рамках схем електронної ідентифікації, щоб розширити транскордонну доступність засобів електронної ідентифікації.

(14) Процес оповіщення про схеми електронної ідентифікації слід спростити та прискорити, щоб сприяти доступу до зручних, надійних, безпечних та інноваційних рішень для автентифікації та ідентифікації та, де це доречно, заохочувати постачальників приватних ідентифікацій пропонувати схеми електронної ідентифікації органам держав-членів для повідомлення про національні схеми електронної ідентифікації особи згідно Регламенту 910/2014.

(15) Впорядкування чинних процедур оповіщення та експертних оглядів запобігає неоднорідним підходам до оцінки різних схем електронної ідентифікації, про які повідомляється, та сприятиме зміцненню довіри між державами-членами. Нові, спрощені

механізми повинні сприяти співробітництву держав-членів щодо безпеки та взаємодії їх заявлених схем електронної ідентифікації.

(16) Держави-члени повинні скористатися новими гнучкими інструментами для забезпечення відповідності вимогам цього Регламенту та відповідних імплементаційних актів. Цей Регламент повинен дозволити державам-членам використовувати звіти та оцінки, що виконуються акредитованими органами з оцінки відповідності, або добровільними схемами сертифікації безпеки інформаційно-комунікаційних технологій, такими як схеми сертифікації, які будуть створені на рівні Союзу відповідно до Регламенту (ЄС) 2019/881, для підтвердження своїх вимог щодо уніфікації схем або їх частин з вимогами Положення про сумісність та безпеку повідомлених схем електронної ідентифікації.

(17) Постачальники послуг використовують ідентифікаційні дані, надані в наборі даних для ідентифікації осіб, доступних із схем електронної ідентифікації відповідно до Регламенту (ЄС) No 910/2014, для встановлення відповідності між користувачами з іншої держави-члена з ідентифікацією цього користувача. Однак, незважаючи на використання набору даних eIDAS, у багатьох випадках забезпечення точної відповідності вимагає додаткової інформації про користувача та конкретних унікальних процедур ідентифікації на національному рівні. Щоб додатково забезпечити зручність використання засобів електронної ідентифікації, цей Регламент повинен вимагати від держав-членів вживати конкретних заходів для забезпечення правильної відповідності особи в процесі електронної ідентифікації. З цією ж метою цей Регламент також повинен розширювати обов'язковий мінімальний набір даних та вимагати використання унікального та постійного електронного ідентифікатора відповідно до законодавства Союзу у тих випадках, коли необхідно в законному порядку ідентифікувати користувача на його/її запит у унікальний і наполегливий спосіб.

(18) Відповідно до Директиви (ЄС) 2019/882, особи з інвалідністю повинні мати можливість користуватися європейськими гарантіями з цифровою ідентичністю, електронними довірчими послугами та продуктами для кінцевих користувачів, які використовуються при наданні цих послуг нарівні з іншими користувачами.

(19) Цей Регламент не повинен охоплювати аспекти, пов'язані з укладанням та чинністю контрактів чи інших юридичних зобов'язань, якщо є вимоги щодо форми, визначеної національним законодавством чи законодавством Союзу. Крім того, це не повинно впливати на вимоги національних форм, що стосуються державних реєстрів, зокрема комерційних та земельних.

(20) Надання та використання електронних довірчих послуг набувають все більшого значення для міжнародної торгівлі та співробітництва. Міжнародні партнери ЄС встановлюють відповідні системи відповідно до положень Регламенту (ЄС) No 910/2014. Тому, щоб полегшити визнання таких послуг та їх постачальників, імплементаційне законодавство може встановити умови, за яких системи цифрової ідентичності третіх країн можна вважати еквівалентними системам для кваліфікованих електронних довірчих послуг та постачальників у цьому Регламенті, як доповнення до можливості взаємного визнання електронних довірчих послуг та постачальників, створених у Союзі та в третіх країнах відповідно до статті 218 Договору.

(21) Цей Регламент повинен спиратися на акти Союзу, що забезпечують конкурентні та чесні ринки у цифровому секторі. Зокрема, він ґрунтується на Регламенті XXX/XXXX

[Закон про цифрові ринки], який запроваджує правила для постачальників основних послуг платформ, призначених як наглядчі шлюзу, і, серед іншого, забороняє наглядчам вимагати від бізнес-користувачів використання, пропонування чи взаємодії зі службою ідентифікації наглядча в контексті послуг, які пропонують бізнес-користувачі, використовуючи основні послуги платформи цього наглядча. Стаття 6 (1) (f) Регламенту XXX/XXXX [Закон про цифрові ринки] вимагає від власників воріт шлюзів дозволити бізнес-користувачам та постачальникам допоміжних послуг про доступ та сумісність з тією самою операційною системою, апаратними чи програмними можливостями, які доступні або використовуються в надання наглядчам шлюзів будь-яких додаткових послуг. Відповідно до статті 15 (15) [Закону про цифрові ринки] послуги ідентифікації є одним із видів додаткових послуг. Тому бізнес-користувачі та постачальники допоміжних послуг повинні мати доступ до таких апаратних чи програмних можливостей, як-от захищених елементів у смартфонах, та взаємодіяти з ними за допомогою Європейських гарантів з цифровою ідентичністю або електронних засобів ідентифікації держав-членів.

(22) Для впорядкування зобов'язань у сфері кібербезпеки, покладених на постачальників електронних довірчих послуг, а також для надання можливості цим постачальникам та їх відповідним компетентним органам скористатися правовою базою, встановленою Директивою XXXX/XXXX (Директива NIS2), електронні довірчі послуги вимагають: вживати відповідних технічних та організаційних заходів відповідно до Директиви XXXX/XXXX (Директива NIS2), таких як заходи щодо усунення системних збоїв, людських помилок, зловмисних дій або природних явищ, з метою управління ризиками, що несуть безпеку мережі та інформаційних систем, які ці провайдери використовувати для надання своїх послуг, а також повідомляти про значні інциденти та кіберзагрози відповідно до Директиви XXXX/XXXX (Директива NIS2). Що стосується повідомлення про інциденти, постачальники електронних довірчих послуг повинні повідомляти про будь-які інциденти, що мають значний вплив на надання їхніх послуг, включаючи такі, викликані крадіжкою або втратою пристроїв, пошкодженням мережевого кабелю або інцидентами, що сталися в контексті ідентифікації осіб. Вимоги щодо управління ризиками кібербезпеки та зобов'язання щодо звітності згідно Директиви XXXXXX [NIS2] слід вважати доповненням до вимог, які пред'являються до постачальників електронних довірчих послуг згідно з цим Регламентом. За необхідності, компетентні органи, призначені відповідно до Директиви XXXX/XXXX, повинні продовжувати застосовувати усталені національні практики чи вказівки щодо впровадження вимог безпеки та звітності та нагляду за дотриманням таких вимог відповідно до Регламенту (ЄС) No 910/2014 (Директива NIS2). Будь-які вимоги відповідно до цього Регламенту не впливають на зобов'язання повідомляти про порушення персональних даних відповідно до Регламенту (ЄС) 2016/679.

(23) Необхідно приділити належну увагу забезпеченню ефективної співпраці між органами NIS та eIDAS. У випадках, коли наглядовий орган згідно з цим Регламентом відрізняється від компетентних органів, призначених відповідно до Директиви XXXX/XXXX [NIS2], ці органи повинні тісно, своєчасно співпрацювати шляхом обміну відповідною інформацією з метою забезпечення ефективного нагляду та дотримання довіри постачальників послуг з вимогами, викладеними у цьому Регламенті та Директиві XXXX/XXXX [NIS2]. Зокрема, наглядові органи відповідно до цього Регламенту повинні мати право вимагати від компетентного органу відповідно до Директиви XXXXX/XXXX [NIS2] надати відповідну інформацію, необхідну для надання статусу кваліфікованого, та здійснювати наглядові дії для перевірки відповідності постачальників електронних довірчих послуг з відповідними вимогами згідно NIS 2 або вимагати їх для усунення невідповідності.

(24) Важливо передбачити законодавчу базу для полегшення транскордонного визнання між існуючими національними правовими системами, що стосуються послуг зареєстрованого постачання даних. Ці рамки також можуть відкрити нові ринкові можливості для постачальників електронних довірчих послуг Союзу пропонувати нові загальноєвропейські послуги з електронного постачання даних та гарантувати, що ідентифікація одержувачів забезпечується з більш високим рівнем впевненості, ніж ідентифікація відправника.

(25) У більшості випадків громадяни та інші мешканці не можуть у цифровому форматі здійснювати транскордонний обмін інформацією, що стосується їх особи, такими як адреси, вік та професійна кваліфікація, посвідчення водія та інші дозволи та платіжні дані, безпечно та з високим рівнем даних захисту.

(26) Має бути можливість видавати та обробляти надійні цифрові документи та сприяти зменшенню адміністративного навантаження, надаючи громадянам та іншим мешканцям можливість використовувати їх у своїх приватних та державних операціях. Громадяни та інші особи, що проживають в ЄС повинні мати можливість, наприклад, продемонструвати право власності на дійсне посвідчення водія, видане органом влади в одній державі-члені, на яке можуть перевірятись та спиратись відповідні органи в інших державах-членах, спиратись на своє соціальне забезпечення облікових даних або майбутніх цифрових проїзних документів у транскордонному контексті.

(27) Будь-яка організація, яка збирає, створює та видає атестаційні документи, такі як дипломи, ліцензії, свідоцтва про народження, повинна мати можливість стати постачальником електронного атестаційного документу. Належні сторони повинні використовувати електронні аверси документації як еквівалентні документам у паперовому форматі. Таким чином, електронний документ не повинен бути визнаним, що втратив в юридичній силі на тій підставі, що він в електронній формі або не відповідає вимогам кваліфікованої електронної атестації документів. З цією метою слід встановити загальні вимоги, щоб гарантувати, що кваліфікована електронна атестація документів має еквівалентну юридичну дію, як і законно видані документи у паперовій формі. Однак ці вимоги повинні застосовуватись без шкоди для законодавства Союзу або національного законодавства, що визначає додаткові вимоги, що стосуються конкретної галузі, щодо форми з юридичними наслідками і, зокрема, транскордонного визнання кваліфікованої електронної атестації документів, де це доречно.

(28) Широка доступність та зручність використання європейських гаманців з цифровою ідентичністю вимагають їх прийняття приватними постачальниками послуг. Приватні сторони, що надають послуги у сферах транспорту, енергетики, банківських та фінансових послуг, соціального забезпечення, охорони здоров'я, питної води, поштових послуг, цифрової інфраструктури, освіти чи телекомунікацій, повинні погодитися на використання європейських гаманців з цифровою ідентичністю для надання послуг, якщо автентифікація користувачів для ідентифікації в Інтернеті вимагається національним законодавством або законодавством Союзу або контрактними зобов'язаннями. Якщо дуже великі онлайн-платформи, як визначено у статті 25.1. Положення [посилання на Положення про DSA] вимагають від користувачів автентифікації для доступу до онлайн-послуг, ці платформи повинні мати повноваження приймати використання європейських гаманців з цифровою ідентичністю на добровільний запит користувача. Користувачі не повинні мати жодних зобов'язань використовувати гаманець для доступу до приватних послуг, але якщо вони цього хочуть, великі онлайн-платформи повинні прийняти для цього Європейських гаманців з цифровою ідентичністю з дотриманням принципу мінімізації даних.

Враховуючи важливість дуже великих онлайн -платформ, через їх охоплення, зокрема виражене в кількості одержувачів послуги та економічних транзакцій, це необхідно для підвищення захисту користувачів від шахрайства та забезпечення високого рівня захисту даних. Кодекси поведінки на рівні Союзу («кодекси поведінки») повинні бути розроблені для того, щоб сприяти широкій доступності та зручності використання засобів електронної ідентифікації, включаючи європейські гарантії з цифровою ідентичністю, у межах цього Регламенту. Кодекси поведінки повинні сприяти широкому прийняттю засобів електронної ідентифікації, включаючи європейські гарантії з цифровою ідентичністю, тих постачальників послуг, які не кваліфікуються як дуже великі платформи і які покладаються на послуги електронної ідентифікації третіх сторін для автентифікації користувачів. Вони повинні бути розроблені протягом 12 місяців після прийняття цього Регламенту. Комісія повинна оцінити ефективність цих положень щодо доступності та зручності використання для користувачів Європейських цифрових гарантіїв після 18 місяців їх розгортання та переглянути положення, щоб забезпечити їх прийняття шляхом делегованих актів у світлі цієї оцінки.

(29) Європейський гаранець з цифровою ідентичністю повинен технічно дозволити вибіркове розкриття документів довіреним сторонам. Ця функція повинна стати базовою функцією дизайну, тим самим посилюючи зручність та захист персональних даних, включаючи мінімізацію обробки персональних даних.

(30) Документи, надані кваліфікованими постачальниками електронних довірчих послуг у рамках кваліфікованої атестації документів, повинні перевірятися на достовірність джерел або безпосередньо кваліфікованим постачальником довірчих послуг, або через призначених посередників, визнаних на національному рівні відповідно до національного законодавства чи законодавства Союзу для мета безпечного обміну атестованими документами між ідентичністю або підтвердження постачальників послуг документів та належних сторін.

(31) Безпечна електронна ідентифікація та надання документів повинні пропонувати додаткову гнучкість та рішення для сектора фінансових послуг, щоб дозволити ідентифікацію клієнтів та обмін конкретними документами, необхідними для виконання, наприклад, вимог належної перевірки клієнтів відповідно до Положення про відмивання грошей [посилання, яке буде додано після прийняття пропозиції], з вимогами щодо придатності, що випливають із законодавства про захист інвесторів, або для підтримки виконання жорстких вимог щодо автентифікації клієнтів для входу в обліковий запис та ініціювання транзакцій у сфері платіжних послуг.

(32) Послуги автентифікації веб-сайту дають користувачам впевненість у тому, що за веб-сайтом стоїть справжня та законна організація. Ці послуги сприяють зміцненню довіри до ведення бізнесу в Інтернеті, оскільки користувачі матимуть довіру до веб-сайту, який був автентифікований. Використання веб-сайтами послуг автентифікації веб-сайтів є добровільним. Однак для того, щоб автентифікація веб-сайту стала засобом підвищення довіри, надання кращого досвіду для користувачів та подальшого зростання на внутрішньому ринку, цей Регламент встановлює мінімальні зобов'язання щодо безпеки та відповідальності для постачальників послуг автентифікації веб-сайтів та їх послуг. З цією метою веб-браузери повинні забезпечувати підтримку та сумісність із Кваліфікованими сертифікатами для автентифікації веб-сайтів відповідно до Регламенту (ЄС) No 910/2014. Вони повинні розпізнавати та відображати кваліфіковані сертифікати для автентифікації веб-сайту, щоб забезпечити високий рівень впевненості, що дозволяє власникам веб-сайтів підтвердити свою особу як власників веб-сайту, а користувачі - з високим ступенем

впевненості. Для подальшого сприяння їх використанню державні органи держав -членів повинні розглянути можливість включення до своїх веб-сайтів кваліфікованих сертифікатів для автентифікації веб-сайтів.

(33) Багато держав-членів запровадили національні вимоги до послуг, що забезпечують безпечне та надійне цифрове архівування, щоб забезпечити довгострокове збереження електронних документів та відповідних довірчих послуг. Для забезпечення юридичної визначеності та довіри важливо забезпечити правову базу для полегшення транскордонного визнання кваліфікованих послуг електронного архівування. Ці рамки також можуть відкрити нові ринкові можливості для постачальників електронних довірчих послуг Союзу.

(34) Кваліфіковані електронні облікові книги реєструють дані таким чином, щоб забезпечити унікальність, достовірність та правильну послідовність записів даних у спосіб захисту від фальсифікацій. Електронна облікова книга об'єднує ефект тимчасового фіксацію даних з упевненістю щодо джерела даних, подібного до електронного підпису, і має додаткову перевагу, дозволяючи використовувати більш децентралізовані моделі управління, які підходять для багатосторонньої співпраці. Наприклад, він створює надійний аудиторський слід для походження товарів у транскордонній торгівлі, підтримує захист прав інтелектуальної власності, забезпечує гнучкість ринків електроенергії, забезпечує основу для прогресивних рішень для цифрової ідентичності та підтримує більш ефективні та трансформаційні державні послуги. Для запобігання фрагментації внутрішнього ринку важливо визначити загальноєвропейську правову базу, яка дозволяє транскордонне визнання електронних довірчих послуг для запису даних в електронних облікових книгах.

(35) Сертифікація як кваліфікованих постачальників електронних довірчих послуг повинна забезпечувати юридичну впевненість у випадках використання, які спираються на електронні облікові книги. Ця послуга для електронних облікових книг та кваліфікованих електронних облікових книг та сертифікація як кваліфікований постачальник електронних довірчих послуг для електронних облікових книг повинні бути незважаючи на необхідність використання випадків відповідності законодавству Союзу або національному законодавству відповідно до законодавства Союзу. Випадки використання, які передбачають обробку персональних даних, повинні відповідати Регламенту (ЄС) 2016/679. Випадки використання, які стосуються криптоактивів повинні бути сумісними з усіма застосовними фінансовими правилами, наприклад, з Директивою про ринки фінансових інструментів, Директивою про платіжні послуги та майбутнім Регламентом про ринки криптоактивів.

(36) Щоб уникнути фрагментації та бар'єрів через різні стандарти та технічні обмеження, а також забезпечити узгоджений процес, щоб уникнути загрози впровадженню майбутньої системи європейської цифрової ідентичності, необхідною є тісна та структурована співпраця між Європейською Комісією, державами-членами та державним і приватним сектором. Для досягнення цієї мети держави-члени повинні співпрацювати в рамках, викладених у Рекомендації Комісії XXX/XXXX [Набір інструментів для скоординованого підходу до Європейської системи цифрової ідентичності], щоб визначити набір інструментів для європейської системи цифрової ідентичності. Набір інструментів повинен містити вичерпну технічну архітектуру та довідкову базу, набір загальних стандартів та технічних посилань та набір керівних принципів та описів найкращих практик, що охоплюють принаймні всі аспекти функціональних можливостей та

сумісності європейських гарантів з цифровою ідентичністю із цифровими ідентифікаторами, включаючи електронні підписи та кваліфіковану електронні довірчі послуги для атестації документів, викладених у цьому регламенті. У цьому контексті держави-члени повинні також досягти згоди щодо спільних елементів бізнес-моделі та структури зборів європейських гарантів з цифровою ідентичністю із цифровою ідентичністю, щоб полегшити залучення, зокрема, малих та середніх компаній у транскордонному контексті. Зміст набору інструментів має розвиватися паралельно та відображати результати обговорення та процесу прийняття Європейської системи цифрової ідентичності.

(37) Згідно з частиною 1 статті 42 Регламенту (ЄС) 2018/1525 Європейського Парламенту та Ради 27 було проведено консультації з Європейським наглядовим органом із захисту даних.

УХВАЛИЛИ ЦЕ ПРАВИЛО:

(1) Статтю 1 викласти у такій редакції:

"Цей Регламент спрямований на забезпечення належного функціонування внутрішнього ринку та забезпечення належного рівня безпеки засобів електронної ідентифікації та електронних довірчих послуг. Для виконання поставлених цілей цей Регламент:

(а) встановлює умови, за яких держави-члени надають та визнають засоби електронної ідентифікації фізичних та юридичних осіб, які підпадають під дію нотифікованої схеми електронної ідентифікації іншої держави-члена;

(б) встановлює правила для електронних довірчих послуг, зокрема для електронних транзакцій;

(с) встановлює нормативно-правову базу для електронних підписів, електронних печаток, електронних позначок часу, електронних документів, електронних послуг реєстрації передачі даних, послуг сертифікації для автентифікації веб-сайтів, електронного архівування та електронного атестації документів, управління пристроями для електронного підпису та створення печаток та електронні облікові книги;

(д) встановлює умови видачі державами-членами європейських гарантів з цифровою ідентичністю;

(2) статтю 2 викласти у такій редакції:

(а) пункт 1 викласти у такій редакції:

‘1. Цей Регламент застосовується до схем електронної ідентифікації, які були повідомлені державою-членом, європейських гарантів з цифровою ідентичністю для цифрової ідентифікації, виданих державами-членами, та до постачальників електронних довірчих послуг, зареєстрованих у Союзі.’;

(б) пункт 3 викласти у такій редакції:

3. Цей Регламент не впливає на національне законодавство чи законодавство Союзу, що стосується укладання та дії договорів чи інших юридичних чи процедурних зобов'язань, що стосуються специфічних галузевих вимог, щодо форми з юридичними наслідками;

(3) статтю 3 викласти у такій редакції:

(а) пункт (2) викласти у такій редакції:

(2) засоби електронної ідентифікації "означають матеріальну та/або нематеріальну одиницю, включаючи Європейські гаманці з цифровою ідентичністю з цифровими ідентифікаторами або посвідчення особи відповідно до Регламенту 2019/1157, що містять дані ідентифікації осіб і які використовуються для автентифікації для онлайн чи офлайн послуг;

(b) пункт (4) викласти у такій редакції:

"(4)" схема електронної ідентифікації "означає систему електронної ідентифікації, за якою засоби електронної ідентифікації видаються фізичним або юридичним особам або фізичним особам, що представляють юридичних осіб";

(c) пункт (14) викласти у такій редакції:

"(14)" сертифікат на електронний підпис "означає електронну атестацію або набір сертифікатів, що пов'язує дані перевірки електронного підпису з фізичною особою та підтверджує принаймні ім'я або псевдонім цієї особи";

(d) пункт (16) викласти у такій редакції:

(16) "електронна довірча послуга" означає електронну послугу, яка зазвичай надається за плату, яка складається з:

(а) створення, перевірка та затвердження електронних підписів, електронних печаток або електронних позначок часу, електронних послуг із реєстрації передачі даних, електронного атестаційного документу та сертифікатів, пов'язаних із цими послугами;

(b) створення, контроль та перевірка сертифікатів для автентифікації веб-сайту;

(c) збереження електронних підписів, печаток або сертифікатів, що стосуються цих послуг;

(d) електронне архівування електронних документів;

(e) управління віддаленими пристроями для створення електронного підпису та печатки;

(f) запис електронних даних до електронної облікової книги;

(e) пункт (21) викласти у такій редакції:

"(21)" продукт "означає апаратне або програмне забезпечення або відповідні компоненти апаратного та/або програмного забезпечення, які призначені для використання для надання послуг електронної ідентифікації та довірчих послуг;

(f) додаються такі пункти (23a) та (23b):

"(23a)" пристрій для створення віддаленого кваліфікованого підпису "означає пристрій для створення кваліфікованого електронного підпису, де кваліфікований постачальник електронних довірчих послуг генерує, керує або дублює дані про створення електронного підпису від імені підписанта;

(23b) "пристрій для створення віддаленої кваліфікованої печатки" означає кваліфікований електронний пристрій створення печатки, де кваліфікований постачальник електронних довірчих послуг генерує, керує або дублює дані про створення електронного підпису від імені автора печатки;

(g) пункт (29) викласти у такій редакції:

"(29)" сертифікат на електронну печатку "означає електронну атестацію або набір сертифікатів, що пов'язує дані валідації електронної печатки з юридичною особою та підтверджує ім'я цієї особи;

(h) пункт (41) викласти у такій редакції:

"(41)" перевірка "означає процес перевірки та підтвердження дійсності електронного підпису або печатки або даних, що посвідчують особу, або електронної атестації документів;

(i) додаються такі пункти (42) - (55):

"(42)" європейський електронний гаманець - це продукт та послуга, яка дозволяє користувачеві зберігати дані, облікові дані та документи, пов'язані з його особистістю, надавати їх належним сторонам за запитом та використовувати їх для автентифікації в Інтернеті та в автономному режимі - за послугу відповідно до статті 6а; а також створити кваліфіковані електронні підписи та печатки;

(43) "документ" - це ознака, характеристика або якість фізичної чи юридичної особи чи юридичної особи в електронній формі;

(44) "електронна атестація документів" - означає атестацію в електронній формі, що дозволяє автентифікувати документи;

(45) "кваліфікована електронна атестація документів" - означає електронну атестацію документів, які видаються кваліфікованим постачальником електронних довірчих послуг та відповідає вимогам, викладеним у Додатку V;

(46) "автентичне джерело" - це сховище чи система, що знаходиться під відповідальністю органу державної влади чи приватної особи, що містить документи про фізичну чи юридичну особу та вважається основним джерелом цієї інформації або визнається автентичним у національному законодавстві;

(47) "електронне архівування" означає послугу, що забезпечує отримання, зберігання, видалення та передачу електронних даних чи документів, щоб гарантувати їх цілісність, точність їх походження та юридичні особливості протягом усього періоду збереження;

(48) "кваліфікована послуга з електронного архівування" означає послугу, яка відповідає вимогам, викладеним у статті 45g;

(49) "відмітка автентичності до гаманця цифрового посвідчення ЄС" означає просте, впізнаване та чітке вказівку на те, що гаманець із цифровим посвідченням особи був випущений відповідно до цього Регламенту;

(50) "автентифікація користувача" означає автентифікацію, засновану на використанні двох або більше елементів, які класифікуються як знання користувачів, володіння та висновки, які є незалежними, таким чином, що порушення одного не порушує надійності інших, і розроблено таким чином для захисту конфіденційності даних автентифікації;

51) "обліковий запис користувача" означає механізм, що дозволяє користувачеві отримувати доступ до державних або приватних послуг на умовах, встановлених постачальником послуг;

(52) "повноваження" означає доказ здібностей, досвіду, права чи дозволу особи;

(53) «електронна облікова книга» означає електронний запис даних, захищений від фальсифікацій, що забезпечує достовірність та цілісність даних, які вони містять, точність їх дати та часу та їх хронологічне впорядкування »;

(54) «персональні дані» означає будь-яку інформацію, визначену у пункті 1 статті 4 Регламенту (ЄС) 2016/679;

(55) "унікальна ідентифікація" означає процес, коли ідентифікаційні дані особи або засоби ідентифікації особи узгоджуються з наявним обліковим записом, що належить тій самій особі, або пов'язані з ними;

(4) Статтю 5 викласти у такій редакції:

"Стаття 5

Псевдоніми в електронних транзакціях

Без шкоди для юридичної сили, наданої псевдонімам відповідно до національного законодавства, використання псевдонімів в електронних транзакціях не забороняється. ';

(5) у главі II заголовок викласти у такій редакції::

Європейські гаманці з цифровою ідентичністю

1. З метою забезпечення того, щоб усі фізичні та юридичні особи в Союзі мали безпечний, надійний та безперебійний доступ до транскордонних державних та приватних послуг, кожна держава-член видає Європейський гаманець із цифровою ідентичністю протягом 12 місяців після набрання чинності цього Регламенту.

2. Європейські гаманці з цифровою ідентичністю видаються:

(a) державою-членом;

(b) за мандатом держави-члена;

(c) незалежно, але визнані державою-членом.

3. Європейські гаманці з цифровою ідентичністю повинні надавати користувачеві можливість:

(a) надійно запитувати та отримувати, зберігати, вибирати, поєднувати та обмінюватись у спосіб, який є прозорим та відстежуваним користувачем, необхідними ідентифікаційними

даними юридичної особи та електронною атестацією документів для автентифікації в онлайн та офлайн для використання онлайн публічних та приватних послуг;
(b) підписувати за допомогою кваліфікованих електронних підписів.

4. Гаманці для цифровою ідентичністю, зокрема:

(a) забезпечити загальний інтерфейс:

(1) кваліфікованим та некваліфікованим постачальникам електронних довірчих послуг, які видають кваліфіковані та некваліфіковані електронні сертифікати документів або інші кваліфіковані та некваліфіковані сертифікати з метою видачі таких атестацій та сертифікатів до європейського гаманця з цифровою ідентичністю;

(2) для належних сторін запитувати та перевіряти ідентифікаційні дані осіб та електронні атестації документів;

(3) для пред'явлення належним сторонам даних ідентифікації осіб, електронного підтвердження документів чи інших даних, таких як облікові дані, у місцевому режимі, що не вимагає доступу до Інтернету для гаманця;

(4) для того, щоб користувач міг дозволити взаємодію з Європейським гаманцем цифрової ідентичності та відобразити відмітку довіри до європейського гаманця цифрової ідентичності»;

(b) забезпечити, щоб постачальники електронних довірчих послуг, які мають кваліфіковані атестації документів, не могли отримати будь-яку інформацію про використання цих документів;

(c) відповідають вимогам, викладеним у статті 8, щодо «високого» рівня впевненості, зокрема стосовно вимог щодо контролю та перевірки ідентичності, а також управління засобами електронної ідентифікації та автентифікації;

(d) забезпечити механізм гарантування того, що належна сторона зможе автентифікувати користувача та отримувати електронні атестації документів;

(e) забезпечити, щоб персональні дані, зазначені у пункті (d) статті 12 (4), однозначно та постійно представляли фізичну чи юридичну особу, пов'язану з ними.

5. Держави-члени надають механізми валідації для європейських гаманців з цифровою ідентичністю:

(a) гарантувати, що його справжність та дійсність можна перевірити;

(b) дозволити належним сторонам перевірити, чи атестації документів є дійсними;

(c) дозволити належним сторонам та кваліфікованим постачальникам електронних електронних довірчих послуг перевірити справжність та дійсність ідентифікаційних даних зазначених осіб.

6. Гаманці європейської цифрової ідентичності видаються згідно із схваленою схемою електронної ідентифікації рівня довіри «високий». Використання Європейських гаманців із цифровою ідентичністю є безкоштовним для фізичних осіб.

7. Користувач повинен повністю контролювати Європейські гаманці з цифровою ідентичністю. Емітент Європейського гаманця цифрової ідентичності не збирає інформацію про використання гаманця, яка не є необхідною для надання послуг гаманця, а також не поєднує ідентифікаційні дані особи та будь-які інші персональні дані, що зберігаються або стосуються використання Європейський гаманець із цифровою ідентичністю з персональними даними будь-яких інших послуг, що пропонуються цим емітентом, або інших послуг, які не потрібні для надання послуг гаманця, якщо користувач не вимагав цього прямо. Персональні дані, що стосуються надання європейських гаманців з цифровою ідентичністю, повинні зберігатися фізично та за логікою окремо від будь-яких інших даних, що зберігаються. Якщо Європейський гаманець з цифровою ідентичністю надається приватними сторонами відповідно до пунктів 1 (b) та (c), положення статті 45f, параграф 4, застосовуються з відповідними змінами.

8. Стаття 11 застосовується *mutatis mutandis* до Європейського гаманця з цифровою ідентичністю.

9. Стаття 24 (2), пункти (b), (e), (g) та (h) застосовуються *mutatis mutandis* до держав-членів, що видають гаманці європейської цифрової ідентичності.

10. Європейський гаманець із цифровою ідентичністю повинен бути доступним для осіб з інвалідністю відповідно до вимог щодо доступності, наведених у Додатку I до Директиви 2019/882.

11. Протягом 6 місяців після набрання чинності цим Регламентом Комісія встановлює технічні та експлуатаційні специфікації та довідкові стандарти для вимог, зазначених у параграфах 3, 4 та 5, за допомогою імплементаційного акта щодо впровадження Європейського гаманця з цифровою ідентичністю. Цей імплементаційний акт приймається відповідно до процедури експертизи, зазначеної у частині 2 статті 48.

Європейські гаманці з цифровою ідентичністю для належних сторін

1. Якщо сторони, що довіряють, мають намір покладатися на Європейські гаманці з цифровою ідентичністю, видані відповідно до цього Регламенту, вони повідомляють про це державі-члену, де зареєстрована довірена сторона, для забезпечення дотримання вимог, викладених у законодавстві Союзу або національному законодавстві щодо забезпечення конкретних послуг. Повідомляючи про свій намір використовувати Європейські гаманці з цифровою ідентичністю, вони також інформують про цільове використання Європейського гаманця з цифровою ідентичністю.

2. Держави-члени впроваджують спільний механізм автентифікації належних сторін

3. Належні сторони несуть відповідальність за проведення процедури автентифікації ідентифікаційних даних осіб та електронної атестації документів, що походять з європейських гаманців з цифровою ідентичністю.

4. Протягом 6 місяців після набрання чинності цим Регламентом Комісія встановлює технічні та експлуатаційні специфікації для вимог, зазначених у параграфах 1 та 2, за допомогою імплементаційного акта щодо впровадження Європейських гаманців для цифрової ідентичності, як зазначено у статті 6а (10).

Стаття 6в

Сертифікація європейських гаманців з цифровою ідентичністю

1. Європейські гаманці з цифровою ідентичністю, які були сертифіковані або для яких було видано декларацію відповідності за схемою кібербезпеки відповідно до Регламенту (ЄС) 2019/881, посилання на які були опубліковані в Офіційному журналі Європейського Союзу, вважатись такими, що відповідають вимогам щодо кібербезпеки, викладеним у пунктах 3, 4 та 5 статті 6а, оскільки сертифікат кібербезпеки або декларація відповідності або їх частини охоплюють ці вимоги.
2. Відповідність вимогам, викладеним у параграфах 3, 4 та 5 статті 6а, що стосуються операцій з обробки персональних даних, що виконуються емітентом Європейських гаманців з цифровою ідентичністю, має бути сертифіковано відповідно до Регламенту (ЄС) 2016/679.
3. Відповідність європейських гаманців з цифровою ідентичністю вимогам, викладеним у пунктах 3, 4 та 5 статті 6а, має бути сертифіковано акредитованими державними чи приватними органами, призначеними державами-членами.
4. Протягом 6 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює перелік стандартів для сертифікації європейських гаманців з цифровою ідентичністю, зазначених у пункті 3.
5. Держави-члени повідомляють Комісії назви та адреси державних або приватних органів, зазначених у пункті 3. Комісія надає цю інформацію державам-членам.
6. Комісія має право приймати делеговані акти відповідно до статті 47 щодо встановлення конкретних критеріїв, яким мають відповідати призначені органи, зазначені у пункті 3.

Стаття 6d

Публікація списку сертифікованих європейських гаманців із цифрової ідентичності

1. Держави -члени невідкладно інформують Комісію про європейські гаманці із цифровою ідентичністю, які були випущені відповідно до статті 6а та сертифіковані органами, зазначеними у пункті 3 статті 6с, вони також негайно інформують Комісію, якщо сертифікація скасовується.
2. На основі отриманої інформації Комісія складає, публікує та підтримує перелік сертифікованих європейських гаманців з цифровою ідентичністю.
3. Протягом 6 місяців після набрання чинності цим Регламентом Комісія визначає формати та процедури, що застосовуються для цілей параграфа 1., за допомогою імплементаційного акта щодо впровадження Європейських гаманців для цифрової ідентичності, як зазначено у статті 6а (10).

(8) перед статтею 7 зазначається такий заголовок:

«РОЗДІЛ II
СХЕМИ ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ»;

(9) вступне речення статті 7 викладено у наступній редакції:

"Відповідно до статті 9 (1) держави-члени повідомляють протягом 12 місяців після набрання чинності цим Регламентом принаймні одну схему електронної ідентифікації, що включає принаймні один засіб ідентифікації;

(10) у статті 9 пункти 2 та 3 замінюються таким:

‘2. Комісія публікує в Офіційному журналі Європейського Союзу перелік схем електронної ідентифікації, які були повідомлені відповідно до пункту 1 цієї статті, та основну інформацію про них.

3. Комісія публікує в Офіційному журналі Європейського Союзу зміни до переліку, зазначеного у пункті 2, протягом одного місяця з дня отримання такого повідомлення;

(11) додається наступна стаття 10а:

"Стаття 10а

Порушення безпеки Європейських гаманців з цифровою ідентичністю

1. Якщо Європейські гаманці з цифровою ідентичністю, видані відповідно до статті 6а та механізми перевірки, зазначені у пунктах (а), (b) та (с) статті 6а (5), порушені або частково скомпрометовані таким чином, що це впливає на їх надійність або надійність інших європейських гаманців із цифровою ідентичністю, держава-емітент негайно призупиняє видачу та скасовує чинність Європейського гаманця з цифровою ідентичністю та інформує про це інші держави-члени та Комісію.

2. У разі усунення порушення або компромісу, зазначеного у пункті 1, держава-член, що видала документи, заново видає та використовує Європейські гаманці з цифровою ідентичністю та негайно інформує про це інші держави-члени та Комісію.

3. Якщо порушення або компроміс, зазначений у пункті 1, не усунеться протягом трьох місяців після призупинення або відкликання, відповідна держава-член вилучає відповідний Європейський гаманець з цифровою ідентичністю та інформує про це інші держави-члени та Комісію. Якщо це виправдано серйозністю порушення, відповідний Європейських гаманців з цифровою ідентичністю негайно вилучається.

4. Комісія негайно публікує в Офіційному журналі Європейського Союзу відповідні зміни до переліку, зазначеного у статті 6d.

5. Протягом 6 місяців після набрання чинності цим Регламентом Комісія додатково визначає заходи, зазначені у параграфах 1 та 3, за допомогою імплементаційного акту щодо впровадження Європейських гаманців з цифровою ідентичністю, як зазначено у статті 6а (10).

(12) додається наступна стаття 11а:

Стаття 11а

Унікальна ідентифікація

1. Коли для автентифікації використовуються нотифіковані засоби електронної ідентифікації та Європейські гаманці з цифровою ідентичністю, держави-члени забезпечують унікальну ідентифікацію.

2. Держави-члени, для цілей цього Регламенту, включають до мінімального набору даних про ідентифікацію осіб, зазначених у статті 12.4 (d), унікальний та постійний ідентифікатор відповідно до законодавства Союзу, щоб ідентифікувати користувача на їх запит у тих випадках, коли ідентифікація користувача вимагається законом.

3. Протягом 6 місяців після набрання чинності цим Регламентом Комісія додатково визначає заходи, зазначені у пунктах 1 та 2, за допомогою імплементаційного акта щодо впровадження Європейських гаманців з цифровою ідентичністю, як зазначено у статті 6а (10).

(13) До статті 12 вносяться такі зміни:

(a) у пункті 3 пункти (c) та (d) виключити;

(b) у пункті 4 пункт (d) викласти у такій редакції:

"(D) посилання на мінімальний набір ідентифікаційних даних осіб, необхідних для однозначного та постійного представлення фізичної чи юридичної особи;

(c) у пункті 6 пункт (a) викласти у такій редакції:

„(A) обмін інформацією, досвідом та передовою практикою щодо схем електронної ідентифікації та, зокрема, технічних вимог, пов'язаних із сумісністю, унікальними рівнями ідентифікації та впевненості;

(14) додається стаття 12а:

Стаття 12а

Сертифікація схем електронної ідентифікації

1. Відповідність повідомлених схем електронної ідентифікації вимогам, викладеним у Статтях 6а, Статті 8 та Статті 10, може бути засвідчена державними або приватними органами, призначеними державами -членами.

2. Вимоги до схем електронної ідентифікації, зазначених у пункті (c) статті 12 (6), не поширюється на схеми електронної ідентифікації або частину таких схем, сертифікованих відповідно до пункту 1. Держави-члени можуть використовувати сертифікат або Декларація про відповідність Союзу, видану відповідно до відповідної європейської схеми сертифікації кібербезпеки, встановленої відповідно до Регламенту (ЄС) 2019/881, щоб продемонструвати відповідність таких схем вимогам, викладеним у статті 8 (2), щодо рівнів довіри у схемах електронної ідентифікації.

3. Держави-члени повідомляють Комісію з інформацією з іменами та адресами державного чи приватного органу, зазначеного у пункті 1. Комісія надає цю інформацію державам-членам;

(15) після статті 12a додається наступний заголовок:

«РОЗДІЛ III

Транскордонна довіра до електронних засобів ідентифікації осіб;

(16) додаються такі статті 12b та 12c:

"Стаття 12b

Транскордонна довіра від європейських гаманців з цифровою ідентичністю

1. Якщо держави-члени вимагають здійснення електронної ідентифікації за допомогою засобів електронної ідентифікації та автентифікації відповідно до національного законодавства або адміністративної практики для доступу до онлайн послуги, що надається органом державної влади, вони також приймають європейські гаманці з цифровою ідентичністю, видані відповідно до цього Регламенту.

2. Якщо до приватних належних сторін, що надають послуги, вимагається національним законодавством або законодавством Союзу, використовувати надійну автентифікацію користувачів для онлайн ідентифікації, або коли автентифікація користувача вимагається за контрактними зобов'язаннями, включаючи сфери транспорту, енергетики, банківських та фінансових послуг, соціальне забезпечення, охорона здоров'я, питна вода, поштові послуги, цифрова інфраструктура, освіта або телекомунікації, приватні належні сторони також погоджуються з використанням європейських гаманців з цифровою ідентичністю, виданих відповідно до статті 6a.

3. Якщо дуже великі онлайн-платформи, як визначено в Регламенті [посилання на Положення про DSA] Стаття 25.1. вимагати від користувачів автентифікації для доступу до онлайн послуг, вони також погоджуються з використанням Європейських гаманців для цифрових ідентифікацій, виданих відповідно до статті 6a, суворо за добровільним запитом користувача та щодо мінімальних документів, необхідних для конкретної онлайн послуги, для якої потрібна автентифікація вимагається, наприклад, підтвердження віку.

4. Комісія заохочує та сприяє розробці кодексів поведінки на рівні Союзу ("кодекси поведінки"), щоб сприяти широкій доступності та зручності використання європейських гаманців з цифровою ідентичністю в межах цього Регламенту. Ці кодекси поведінки забезпечують прийняття засобів електронної ідентифікації, включаючи європейські гаманці цифрової ідентифікації, у межах цього Регламенту, зокрема постачальниками послуг, які покладаються на послуги електронної ідентифікації третіх сторін для автентифікації користувачів. Комісія сприятиме розробці таких кодексів поведінки у тісній співпраці з усіма відповідними зацікавленими сторонами та заохочуватиме постачальників послуг завершити розробку кодексів поведінки протягом 12 місяців після прийняття цього Регламенту та ефективно впровадити їх протягом 18 місяців після прийняття Регламенту.

5. Комісія протягом 18 місяців після впровадження Європейських гаманців цифрової ідентичності оцінює на підставі доказів, що свідчать про наявність та зручність використання Європейського гаманця з цифровою ідентичністю, додаткові приватні постачальники онлайн послуг мають прийняти використання Європейських гаманців з цифровою ідентичністю чітко за добровільним запитом користувача. Критерії оцінки

можуть включати обсяг бази користувачів, транскордонну присутність постачальників послуг, технологічний розвиток, еволюцію моделей використання. Комісія має право приймати делеговані акти на основі цієї оцінки щодо перегляду вимог щодо визнання Європейського гаманця з цифровою ідентичністю відповідно до пунктів 1-4 цієї статті.

6. Для цілей цієї статті на європейські гаманці з цифровою ідентичністю не поширюються вимоги, зазначені у статтях 7 та 9.

Стаття 12в

Взаємне визнання інших засобів електронної ідентифікації

1. Якщо електронна ідентифікація за допомогою засобів електронної ідентифікації та автентифікації вимагається згідно з національним законодавством або адміністративною практикою для доступу до онлайн послуги, що надається органом державної влади держави-члена, засоби електронної ідентифікації, видані в іншій державі-члені, визнаються у першій державі-члені для цілей транскордонної автентифікації для цієї онлайн-послуги за умови дотримання таких умов:

(а) засоби електронної ідентифікації видаються за схемою електронної ідентифікації, яка включена до переліку, зазначеного у статті 9;

(б) рівень довіри до засобів електронної ідентифікації відповідає рівню довіри, ідентичному або вищому за рівень довіри, необхідний відповідному органу державної влади для доступу до цієї онлайн послуги у відповідній державі-члені, і в будь-якому випадку не нижче рівня довіри «значний»;

(с) відповідний орган державної влади у державі-члені використовує рівень довіри "значний" або "високий" щодо доступу до цієї онлайн послуги.

Таке визнання має відбутися не пізніше ніж через 6 місяців після того, як Комісія опублікує перелік, зазначений у пункті (а) першого підпункту.

2. Засоби електронної ідентифікації, які видаються в межах схеми електронної ідентифікації, включеної до переліку, зазначеного у статті 9, і який відповідає рівню довіри "низький", можуть бути визнані органами державної влади для цілей транскордонного автентифікації для онлайн послуг, що надаються цими органами;

(17) У статті 13 параграф 1 викласти у наступній редакції:

‘1. Незважаючи на пункт 2 цієї статті, постачальники електронних електронних довірчих послуг несуть відповідальність за шкоду, завдану навмисно чи з необережності будь-якій фізичній чи юридичній особі через невиконання зобов’язань за цим Регламентом та зобов’язань щодо управління ризиками кібербезпеки згідно зі статтею 18 Директиви. XXXX/XXXX [NIS2];

(18) Статтю 14 викласти у наступній редакції:

"Стаття 14

Міжнародні аспекти

1. Комісія може прийняти імплементаційні акти відповідно до статті 48 (2), що визначають умови, за яких вимоги третьої країни, що застосовуються до постачальників електронних довірчих послуг, які мають свою територію, та до електронних довірчих послуг, які вони надають, можуть розглядатися еквівалентні вимогам, що застосовуються до постачальників кваліфікованих електронних довірчих послуг, зареєстрованих у Союзі, та до кваліфікованих електронних довірчих послуг, які вони надають.

2. Якщо Комісія прийняла імплементаційний акт відповідно до пункту 1 або уклала міжнародну угоду про взаємне визнання електронних довірчих послуг відповідно до статті 218 Договору, електронні довірчі послуги, що надаються постачальниками із відповідної третьої країни, вважаються еквівалентними кваліфікованим електронним довірчим послугам, що надаються кваліфікованими постачальниками електронних довірчих послуг, зареєстрованими у Союзі. ';

(19) Статтю 15 викласти у наступній редакції:

Стаття 15

Доступність для людей з інвалідністю

Надання електронних довірчих послуг та продуктів для кінцевих споживачів, що використовуються при наданні цих послуг, має бути доступним для осіб з інвалідністю відповідно до вимог щодо доступності Додатка I Директиви 2019/882 щодо вимог доступності для продуктів та послуг. ';

(20) До статті 17 вносяться наступні зміни:

(a) пункт 4 викласти у наступній редакції:

(1) пункт (с) пункту 4 викласти у наступній редакції:

'(с) інформувати відповідні національні компетентні органи відповідних держав-членів, призначені згідно з Директивою (ЄС) XXXX/XXXX [NIS2], про будь-які значні порушення безпеки або втрату довіри, про які вони дізнаються під час виконання своїх завдань. якщо суттєве порушення безпеки або втрата довіри стосується інших держав-членів, наглядовий орган повідомляє єдину контактну особу відповідної держави-члена, призначену відповідно до Директиви (ЄС) XXXX/XXXX (NIS2); “;

(2) пункт (f) викласти у наступній редакції:

'(f) співпрацювати з наглядовими органами, створеними відповідно до Регламенту (ЄС) 2016/679, зокрема, негайно інформуючи їх про результати перевірок кваліфікованих постачальників електронних довірчих послуг, де були порушені правила захисту персональних даних та порушення безпеки, що є порушенням персональних даних; ';

(b) пункт 6 замінюється таким:

'6. Щороку до 31 березня кожен наглядовий орган подає Комісії звіт про свою основну діяльність протягом попереднього календарного року;

(с) пункт 8 викласти у наступній редакції:

‘8. Протягом 12 місяців після набрання чинності цим Регламентом Комісія за допомогою актів імплементації додатково визначає завдання наглядових органів, зазначених у пункті 4, та визначає формати та процедури звіту, зазначеного у пункті 6. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2).’;

(21) До статті 18 вносяться такі зміни:

(а) заголовок статті 18 замінюється таким:

"Взаємодопомога та співпраця";

(b) пункт 1 замінюється таким:

‘1. Наглядові органи повинні співпрацювати з метою обміну передовою практикою та інформацією щодо надання електронних довірчих послуг;

(с) додаються такі пункти 4 та 5:

‘4. Наглядові органи та національні компетентні органи відповідно до Директиви (ЄС) XXXX/XXXX Європейського Парламенту та Ради [NIS2] повинні співпрацювати та допомагати один одному для забезпечення дотримання постачальниками електронних довірчих послуг вимог, викладених у цьому Регламенті та Директиві (ЄС) XXXX/XXXX [NIS2]. Наглядовий орган вимагає від національного компетентного органу відповідно до Директиви XXXX/XXXX [NIS2] здійснити наглядові дії для перевірки відповідності постачальників електронних довірчих послуг вимогам Директиви XXXX/XXXX (NIS2), щоб вимагати від постачальників електронних довірчих послуг виправлення будь-яке невиконання цих вимог, своєчасне надання результатів будь-якої наглядової діяльності, пов'язаної з постачальниками електронних довірчих послуг, та інформування наглядових органів про відповідні інциденти, повідомлені відповідно до Директиви XXXX/XXXX [NIS2].

5. Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює необхідні процедурні механізми для полегшення співпраці між наглядовими органами, зазначеними у пункті 1. “;

(22) До статті 20 вносяться наступні зміни:

(а) пункт 1 викласти у наступній редакції:

‘1. Кваліфіковані постачальники електронних довірчих послуг перевіряються за свій рахунок щонайменше кожні 24 місяці органом з оцінки відповідності. аудит повинен підтвердити, що кваліфіковані постачальники електронних довірчих послуг та надані ними кваліфіковані електронні довірчі послуги відповідають вимогам, викладеним у цьому Регламенті та у статті 18 Директиви (ЄС) XXXX/XXXX [NIS2]. кваліфіковані постачальники електронних довірчих послуг подають отриманий звіт про оцінку відповідності до наглядового органу протягом трьох робочих днів з дня його отримання.’;

(b) в пункті 2 останнє речення замінено наступним:

"Якщо правила захисту персональних даних виявляються порушеними, наглядовий орган інформує наглядові органи відповідно до Регламенту (ЄС) 2016/679 про результати своїх аудитів;

(с) параграфи 3 та 4 викласти у наступній редакції:

‘3. Якщо кваліфікований постачальник електронних довірчих послуг не виконує будь-яку з вимог, викладених у цьому Регламенті, наглядовий орган вимагає від нього компенсацію у встановлений термін, якщо це можливо.

якщо цей постачальник не надає компенсацію у строк, встановлений наглядовим органом, наглядовий орган, беручи до уваги, зокрема, ступінь, тривалість та наслідки цієї помилки, може відкликати кваліфікаційний статус цього постачальника або щодо відповідної послуги, яку він надає, та вимагати від нього, де це можливо, протягом встановленого терміну виконання вимог Директиви XXXX/XXXX [NIS2]. Наглядовий орган інформує орган, зазначений у частині 3 статті 22, з метою оновлення довірених списків, зазначених у частині 1 статті 22.

Наглядовий орган інформує кваліфікованого постачальника електронних довірчих послуг про відкликання його кваліфікаційного статусу або кваліфікаційного статусу відповідної послуги.

4. Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює довідковий номер для таких стандартів:

(а) акредитацію органів з оцінки відповідності та звіт про оцінку відповідності, зазначений у пункті 1;

(б) вимоги аудиту до органів з оцінки відповідності для здійснення ними оцінки відповідності кваліфікованих постачальників електронних довірчих послуг, як зазначено у пункті 1, що проводиться органами з оцінки відповідності;

(с) схеми оцінки відповідності для проведення оцінки відповідності кваліфікованих постачальників електронних довірчих послуг органами з оцінки відповідності та надання звіту про оцінку відповідності, зазначеного у пункті 1.

Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ‘;

(23) До статті 21 вносяться такі зміни:

(а) пункт 2 викласти у наступній редакції:

‘2. Наглядовий орган перевіряє, чи постачальник електронних довірчих послуг та надані ним електронні довірчі послуги відповідають вимогам, викладеним у цьому Регламенті, і, зокрема, вимогам до кваліфікованих постачальників електронних довірчих послуг та до кваліфікованих довірчих послуг, які вони надають.

Для того, щоб перевірити відповідність постачальника електронних довірчих послуг вимогам, викладеним у статті 18 Директиви XXXX [NIS2], наглядовий орган вимагає від компетентних органів, зазначених у Директиві XXXX [NIS2], здійснити наглядові дії щодо цього та надати інформацію про результати протягом трьох днів з моменту їх завершення.

Якщо наглядовий орган дійшов висновку, що постачальник електронних довірчих послуг та надані ним електронні довірчі послуги відповідають вимогам, зазначеним у першому підпункті, наглядовий орган надає кваліфікований статус постачальнику електронних довірчих послуг та наданим ним довірчим послугам та інформує про це орган зазначених у частині 3 статті 22 з метою оновлення довірених списків, зазначених у статті 22 (1), не пізніше ніж через три місяці після повідомлення відповідно до пункту 1 цієї статті.

Якщо перевірка не завершується протягом трьох місяців з моменту повідомлення, наглядовий орган повідомляє постачальника електронних довірчих послуг із зазначенням причин затримки та строку, протягом якого перевірка має бути завершена;

(b) пункт 4 викласти у наступній редакції:

‘4. Протягом 12 місяців після набрання чинності цим Регламентом Комісія за допомогою актив-імплементатії визначає формати та процедури повідомлення та перевірки для цілей пунктів 1 та 2 цієї статті. Ці імплементатійні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ‘;

(24) у статті 23 додається наступний пункт 2a:

‘2a. Параграфи 1 та 2 також застосовуються до постачальників електронних довірчих послуг, що мають місцезнаходження у третіх країнах, та до послуг, які вони надають, за умови, що вони були визнані в Союзі відповідно до статті 14. ‘;

(25) До статті 24 вносяться такі зміни:

(a) пункт 1 викласти у наступній редакції:

‘1. Видаючи кваліфікований сертифікат або кваліфіковане електронне підтвердження документів для електронних довірчих послуг, кваліфікований постачальник електронних довірчих послуг перевіряє особу та, у разі необхідності, будь-які документи фізичної чи юридичної особи, якій належить кваліфікований сертифікат або кваліфікована електронна атестація документа видається.

Інформація, зазначена у першому підпункті, перевіряється кваліфікованим постачальником електронних довірчих послуг або безпосередньо, або спираючись на третю сторону будь-яким із наведених нижче способів:

(a) за допомогою засобів електронної ідентифікації, про які повідомляється, які відповідають вимогам, викладеним у статті 8, щодо рівнів довіри "значний" або "високий";
(b) за допомогою кваліфікованих електронних підтверджень документів або сертифіката кваліфікованого електронного підпису або кваліфікованої електронної печатки, виданого відповідно до пунктів (a), (c) або (г);

(c) шляхом використання інших методів ідентифікації, які забезпечують ідентифікацію фізичної особи з високим рівнем впевненості, відповідність якої підтверджується органом з оцінки відповідності;

(d) шляхом фізичної присутності особи або уповноваженого представника юридичної особи за відповідними процедурами та відповідно до національного законодавства, якщо інші засоби відсутні;

(b) додається такий параграф 1a:

‘1a. Протягом 12 місяців після набрання чинності цим Регламентом Комісія за допомогою імплементаційних актів визначає мінімальні технічні специфікації, стандарти та процедури щодо перевірки ідентичності та документів відповідно до пункту с пункту 1. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2).’;

(c) пункт 2 викласти у наступній редакції:

(1) пункт (d) викласти у наступній редакції:

‘(d) перед вступом у договірні відносини повідомляти у чіткій, всебічній та легкодоступній спосіб у загальнодоступному просторі та окремо будь-яку особу, яка прагне скористатися кваліфікованою електронною довірчою послугою

(2) додаються параграфи (fa) та (fb):

"(Fa) мати відповідну політику та вживати відповідних заходів для управління юридичними, господарськими, операційними та іншими прямими чи непрямими ризиками для надання кваліфікованої електронної довірчої послуги. Незважаючи на положення статті 18 Директиви EU XXXX/XXX [NIS2], ці заходи повинні включати принаймні наступне:

(i) заходи, пов'язані з реєстрацією та процедурою надання послуги;

(ii) заходи, пов'язані з процедурними або адміністративними перевітками;

(iii) заходи, пов'язані з управлінням та впровадженням послуг.

(fb) повідомляти наглядовий орган та, у разі необхідності, інші відповідні органи про будь-які пов'язані порушення у здійсненні заходів, зазначених у пункті (i), (ii) та (iii) пункту (fa), значний вплив на надану електронну довірчу послугу або на персональні дані, які там зберігаються.’;

(3) пункти (g) та (h) замінюються таким:

"(G) вживати відповідних заходів щодо підробки, крадіжки чи привласнення даних або, без права, видалення, зміни або відсутності доступу до даних;

(h) реєструвати та зберігати доступ до тих пір, поки це буде необхідно після припинення діяльності кваліфікованого постачальника електронних довірчих послуг, всю відповідну інформацію щодо даних, виданих та отриманих кваліфікованим постачальником довірчих

послуг, з метою надання доказів у судових розглядах та для мета забезпечення безперервності обслуговування. Такий запис може здійснюватися в електронному вигляді;

(4) пункт (j) виключено;

(d) додається такий параграф 4а:

‘4а. Параграфи 3 та 4 відповідно застосовуються до скасування електронних атестатів документів;

(е) пункт 5 викласти у наступній редакції:

‘5. Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює порядкові номери стандартів для вимог, зазначених у пункті 2. Відповідність вимогам, викладеним у цій статті, передбачається, якщо надійні системи та продукти відповідають цим стандартам. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ‘;

(f) додається такий пункт 6:

‘6. Комісія має право приймати делеговані акти щодо додаткових заходів, зазначених у пункті 2 (fa). ‘;

(26) У статті 28 параграф 6 замінюється таким:

‘6. Протягом 12 місяців після набрання чинності цим Регламентом Комісія за допомогою імплементаційних актів встановлює порядкові номери стандартів для кваліфікованих сертифікатів для електронного підпису. Виконання вимог, викладених у Додатку I, передбачається, якщо кваліфікований сертифікат на електронний підпис відповідає цим стандартам. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ‘;

(27) У статті 29 додається наступний новий пункт 1а:

‘1а. Створення, управління та копіювання даних про створення електронного підпису від імені підписанта може здійснюватись лише кваліфікованим постачальником електронних довірчих послуг, який надає кваліфіковану електронну довірчу послугу для управління віддаленим пристроєм для створення електронного підпису. ‘;

(28) додається наступна стаття 29а:

"Стаття 29а

Вимоги до кваліфікованої послуги з управління віддаленими пристроями створення електронного підпису

1. Керування віддаленими пристроями створення електронного підпису як кваліфікованою послугою може здійснюватись лише кваліфікованим постачальником електронних довірчих послуг, який:

(a) формує або керує даними щодо створення електронного підпису від імені підписанта;

(b) незважаючи на пункт (1) (d) Додатка II, дублює дані про створення електронного підпису лише для резервного копіювання за умови дотримання таких вимог:

безпека дубльованих наборів даних повинна бути на тому ж рівні, що і для вихідних наборів даних;

кількість дубльованих наборів даних не повинна перевищувати мінімум, необхідний для забезпечення безперервності обслуговування.

(с) відповідає будь-яким вимогам, визначеним у звіті про сертифікацію конкретного пристрою для створення віддаленого кваліфікованого підпису, виданому відповідно до статті 30.

(29) У статтю 30 додається наступний пункт 3а:

‘3а. Сертифікат, зазначений у пункті 1, діє протягом 5 років, залежно від регулярної 2-річної оцінки вразливості. У разі виявлення вразливих місць та їх усунення сертифікат відкликається. ‘;

(30) У статті 31 параграф 3 замінюється таким:

‘3. Протягом 12 місяців після набрання чинності цим Регламентом Комісія за допомогою актив-імплементатії визначає формати та процедури, що застосовуються для цілей параграфа 1. Ці імплементатійні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ‘;

(31) У статтю 32 вносяться такі зміни:

(а) у пункті 1 додається такий підпункт:

"Виконання вимог, викладених у першому підпункті, передбачається, якщо перевірка кваліфікаційних електронних підписів відповідає стандартам, зазначеним у пункті 3;

(b) пункт 3 викласти у наступній редакції:

‘3. Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження активів встановлює порядкові номери стандартів для валідації кваліфікованих електронних підписів. Ці імплементатійні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ‘;

(32) Статтю 34 викласти у наступній редакції:

Стаття 34

Кваліфікована послуга збереження кваліфікованих електронних підписів

1. Кваліфіковану послугу збереження кваліфікованих електронних підписів може надавати лише кваліфікований постачальник електронних довірчих послуг, який використовує процедури та технології, здатні розширити надійність кваліфікованого електронного підпису після закінчення терміну їх дії.

2. Виконання вимог, викладених у пункті 1, передбачається, якщо домовленості щодо кваліфікованої послуги збереження кваліфікованих електронних підписів відповідають стандартам, зазначеним у пункті 3.

3. Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює порядкові номери стандартів для кваліфікованої послуги збереження для кваліфікованих електронних підписів. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ';

(33) До статті 37 вносяться такі зміни:

(a) додається наступний параграф 2a:

‘2a. Виконання вимог щодо вдосконалених електронних печаток, зазначених у статті 36 та пункті 5 цієї статті, передбачається, якщо вдосконалена електронна печатка відповідає стандартам, зазначеним у пункті 4;

(b) пункт 4 викласти у наступній редакції:

‘4. Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює порядкові номери стандартів для сучасних електронних печаток. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ';

(34) До статті 38 вносяться такі зміни:

(a) пункт 1 викласти у наступній редакції:

‘1. Кваліфіковані сертифікати на електронні печатки повинні відповідати вимогам, викладеним у Додатку III. Виконання вимог, викладених у Додатку III, передбачається, якщо кваліфікований сертифікат на електронну печатку відповідає стандартам, зазначеним у пункті 6. “;

(b) пункт 6 викласти у наступній редакції:

‘6. Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює порядкові номери стандартів для кваліфікованих сертифікатів для електронних печаток. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ';

(35) додається наступна стаття 39a:

Стаття 39a

Вимоги до кваліфікованої послуги управління віддаленими пристроями для створення електронних печаток

Стаття 29a застосовується *mutatis mutandis* до кваліфікованої послуги управління віддаленими пристроями для створення електронних печаток;

(36) До статті 42 вносяться такі зміни:

(a) додається наступний новий пункт 1a:

‘1а. Виконання вимог, викладених у пункті 1, передбачається, коли прив’язка дати та часу до даних та точного джерела часу відповідає стандартам, зазначеним у пункті 2;

(b) пункт 2 викласти у наступній редакції:

‘2. Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює порядкові номери стандартів для прив’язки дати та часу до даних та для точних джерел часу. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ‘;

(37) До статті 44 вносяться такі зміни:

(a) додається наступний параграф 1а:

‘1а. Виконання вимог, викладених у пункті 1, передбачається, коли процес надсилання та отримання даних відповідає стандартам, зазначеним у пункті 2;

(b) пункт 2 викласти у наступній редакції:

‘2. Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює порядкові номери стандартів для процесів надсилання та отримання даних. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ‘;

Статтю 45 замінено таким:

Стаття 45

Вимоги до кваліфікованих сертифікатів для автентифікації веб –сайту

1. Кваліфіковані сертифікати для автентифікації веб-сайту повинні відповідати вимогам, викладеним у Додатку IV. Кваліфіковані сертифікати для автентифікації веб-сайту вважаються такими, що відповідають вимогам, викладеним у Додатку IV, якщо вони відповідають стандартам, зазначеним у пункті 3.

2. Кваліфіковані сертифікати для автентифікації веб-сайту, зазначені у пункті 1, визнаються веб-браузерами. Для цих цілей веб-браузери повинні гарантувати, що дані особи, надані будь-яким із методів, відображаються зручним для користувача способом. Веб-браузери повинні забезпечувати підтримку та сумісність із кваліфікованими сертифікатами для автентифікації веб-сайтів, зазначених у пункті 1, за винятком підприємств, які вважаються мікропідприємствами та малими підприємствами відповідно до Рекомендації Комісії 2003/361/ЄС у перші 5 років функціонування як постачальники послуг перегляду веб-сторінок.

3. Протягом 12 місяців після набрання чинності цим Регламентом Комісія за допомогою актів імплементації надає специфікації та порядкові номери стандартів для кваліфікованих сертифікатів для автентифікації веб –сайтів, зазначених у пункті 1. Ці імплементаційні акти мають бути прийняті, відповідно до процедури експертизи, зазначеної у статті 48 (2);

(39) наступні розділи 9, 10 та 11 додаються після статті 45;

«РОЗДІЛ 9

ЕЛЕКТРОННА АТЕСТАЦІЯ ДОКУМЕНТІВ

Стаття 45a

Правові наслідки електронна атестація документів

1. Електронній атестації документів не може бути відмовлено у юридичній силі та допустимості як доказ у судовому розгляді виключно на тій підставі, що вона в електронному вигляді.
2. Кваліфікована електронна атестація документів має таку ж юридичну дію, що і законно видані документи в паперовій формі.
3. Кваліфікована електронна атестація документів, видана в одній державі-члені, визнається кваліфікованою електронною атестацією документів у будь-якій іншій державі-члені.

Стаття 45b

Електронна атестація документів під чам надання публічних послуг

Коли для доступу до онлайн послуги, що надається органом державної влади, відповідно до національного законодавства потрібна електронна ідентифікація за допомогою засобів електронної ідентифікації та автентифікації, ідентифікаційні дані особи в електронному підтвердженні документів не замінюють електронну ідентифікацію за допомогою засобів електронної ідентифікації та автентифікації для здійснення електронної ідентифікації, якщо це не дозволено державою-членом або органом державної влади. У такому випадку також приймається кваліфікована електронна атестація документів інших держав-членів.

Стаття 45в

Вимоги до кваліфікованої атестації документів

1. Кваліфікована електронна атестація документів повинна відповідати вимогам, викладеним у Додатку V. Кваліфікована електронна атестація документів вважається такою, що відповідає вимогам, викладеним у Додатку V, якщо вона відповідає стандартам, зазначеним у пункті 4.
2. Кваліфікована електронна атестація документів не підлягає встановленню жодних обов'язкових вимог на додаток до вимог, викладених у Додатку V.
3. Якщо кваліфіковану електронну атестацію документів було скасовано після первинної видачі, вона втрачає чинність з моменту її відкликання, і її статус ні за яких обставин не може бути скасовано.
4. Протягом 6 місяців після набрання чинності цим Регламентом Комісія встановлює порядкові номери стандартів для кваліфікованої електронної атестації документів за допомогою імплементаційного акта щодо впровадження Європейських гарантів для цифрової ідентичності, як зазначено у статті 6a (10).

Стаття 45д

Перевірка документів у достовірних джерелах

1. Держави-члени забезпечують, щоб, принаймні щодо документів, перелічених у Додатку VI, там, де ці документи спираються на достовірні джерела у публічному секторі, вживалися заходи, що дозволяють кваліфікованим постачальникам електронних атестатів документів перевіряти їх електронними засобами на запит користувача, автентичність документа безпосередньо до відповідного автентичного джерела на національному рівні або через призначених посередників, визнаних на національному рівні відповідно до національного законодавства чи законодавства Союзу.

2. Протягом 6 місяців після набрання чинності цим Регламентом, з урахуванням відповідних міжнародних стандартів, Комісія визначає мінімальні технічні специфікації, стандарти та процедури з посиланням на каталог документів та схем для документів та перевірки процедури кваліфікованої електронної атестації документів за допомогою імплементаційного акта щодо впровадження Європейських гарантів цифрової ідентичності, як зазначено у статті 6а (10).

Стаття 45е

Видача електронних атестатів документів для Європейських гарантів з цифровою ідентичністю

Постачальники кваліфікованих електронних атестатів документів мають надати інтерфейс із гарантими європейської цифрової ідентичності, виданими відповідно до статті 6а.

Стаття 45f

Додаткові правила надання послуг електронної атестації документів

1. Постачальники кваліфікованої та некваліфікованої електронної сертифікації атестації документів не повинні поєднувати персональні дані, що стосуються надання цих послуг, з персональними даними будь-яких інших послуг, які вони пропонують.

2. Персональні дані, що стосуються надання послуг з електронної атестації документів, повинні зберігатися окремо від інших даних, що зберігаються.

3. Персональні дані, що стосуються надання кваліфікованих послуг з електронної атестації документів, повинні зберігатися фізично та логічно окремо від будь-яких інших даних, що зберігаються.

4. Постачальники кваліфікованої кваліфікованих послуг з електронної атестації документів надають такі послуги юридичній особі.

РОЗДІЛ 10

КВАЛІФІКОВАНІ ПОСЛУГИ ЕЛЕКТРОННОГО АРХІВУВАННЯ

Стаття 45g

Кваліфіковані послуги електронного архівування

Кваліфіковану послугу електронного архівування електронних документів може надавати лише кваліфікований постачальник електронних довірчих послуг, який використовує процедури та технології, здатні розширити надійність електронного документа після закінчення терміну їх дії.

Протягом 12 місяців після набрання чинності цим Регламентом Комісія шляхом впровадження актів встановлює порядкові номери стандартів для послуг електронного архівування. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у частині 2 статті 48.

РОЗДІЛ 11

Електронні облікові книги

Стаття 45h

Правові наслідки електронних облікових книг

1. Електронний обліковий книзі не можна відмовляти в юридичній силі та допустимості як доказ в судовому процесі лише на тій підставі, що вона в електронній формі або не відповідає вимогам щодо кваліфікованих електронних облікових книг.
2. Кваліфікована електронна облікова книга має користуватися припущенням про унікальність та достовірність даних, які вони містять, про точність їх дати та часу, а також про їх послідовне хронологічне впорядкування у книзі обліку.

Стаття 45i

Вимоги до кваліфікованих електронних облікових книг

1. Кваліфіковані електронні облікові книги повинні відповідати таким вимогам:

- (a) вони створені одним або кількома кваліфікованими постачальниками або постачальниками електронних довірчих послуг;
- (b) вони забезпечують унікальність, достовірність та правильну послідовність записів даних, записаних у книзі обліку;
- (c) вони забезпечують правильне послідовне хронологічне впорядкування даних у книзі обліку та точність дати та часу введення даних;
- (d) вони зберігають дані таким чином, щоб будь-яка подальша зміна даних була негайно виявлена.

2. Виконання вимог, викладених у пункті 1, вважається, якщо електронна облікова книга відповідає стандартам, зазначеним у пункті 3.

3. Комісія може за допомогою актів імплементації встановити порядкові номери стандартів для процесів виконання та реєстрації набору даних та створення кваліфікованої електронної облікової книги. Ці імплементаційні акти приймаються відповідно до процедури експертизи, зазначеної у статті 48 (2). ';

(40) Додається наступна стаття 48а:

Стаття 48а

Вимоги до звітності

1. Держави-члени забезпечують збір статистичних даних щодо функціонування Європейських гаманців цифрової ідентичності та кваліфікованих електронних довірчих послуг.
2. Статистичні дані, зібрані відповідно до пункту 1, включають наступне:
 - (а) кількість фізичних та юридичних осіб, які мають дійсний Європейський гаманець з цифровою ідентичністю;
 - (б) тип та кількість послуг, що приймають використання Європейського гаманця з цифровою ідентичністю;
 - (в) інциденти та час простою інфраструктури на національному рівні, що перешкоджає використанню програм Європейського гаманця з цифровою ідентичністю.
3. Статистичні дані, зазначені у пункті 2, мають бути доступними для громадськості у відкритому та загальнодоступному машиночитаному форматі.
4. Щороку до березня держави-члени подають Комісії звіт про статистику, зібрану відповідно до параграфа 2.;

(41) Статтю 49 викласти у наступній редакції:

Стаття 49

Огляд

1. Комісія розглядає застосування цього Регламенту та звітує перед Європейським Парламентом та Радою протягом 24 місяців після набрання ним чинності. Комісія оцінює, зокрема, чи доцільно змінювати сферу застосування цього Регламенту або його конкретних положень, беручи до уваги досвід, набутий у застосуванні цього Регламенту, а також технологічні, ринкові та правові зміни. За необхідності до цього звіту додається пропозиція щодо внесення змін до цього Регламенту.
2. Звіт про оцінку повинен містити оцінку доступності та зручності використання засобів ідентифікації, включаючи Європейські гаманці з цифровою ідентичністю, що підпадають під сферу застосування цього Регламенту, та оцінювати, чи мають усі постачальники послуг приватної мережі, які покладаються на послуги електронної ідентифікації третіх осіб для автентифікації користувачів, мати обов'язок прийняти використання повідомлених засобів електронної ідентифікації та європейські
3. Крім того, Комісія подає Європейському Парламенту та Раді звіт кожні чотири роки після звіту, зазначеного у першому параграфі, про прогрес у досягненні цілей цього Регламенту.

(42) Статтю 51 викласти у наступній редакції:
Стаття 51

Перехідні заходи

1. Пристрої створення безпечних підписів, відповідність яких визначена відповідно до статті 3 (4) Директиви 1999/93/ЄС, продовжуватимуть вважатися кваліфікованими пристроями для створення електронного підпису відповідно до цього Регламенту до [дата, будь ласка, вставте період чотири роки після набрання чинності цим Регламентом].

2. Кваліфіковані сертифікати, видані фізичним особам відповідно до Директиви 1999/93/ЄС, продовжуватимуть вважатися кваліфікованими сертифікатами для електронних підписів згідно з цим Регламентом до [будь ласка, вставте період у чотири роки після набрання чинності цим Регламентом].

(43) Додаток I змінюється відповідно до Додатка I до цього Регламенту;

(44) Додаток II замінюється текстом, викладеним у Додатку II до цього Регламенту;

(45) Додаток III змінюється відповідно до Додатку III до цього Регламенту;

(46) Додаток IV змінюється відповідно до Додатку IV до цього Регламенту;

(47) додається новий Додаток V, викладений у Додатку V до цього Регламенту;

(48) до цього Регламенту додається новий Додаток VI.

Стаття 2

Цей Регламент набирає чинності на двадцятий день після його опублікування в Офіційному віснику Європейського Союзу.

Цей Регламент є обов'язковим у своїй повноті та безпосередньо застосовується у всіх державах-членах.

Прийнято у Брюсселі,