Official Journal
of the European Union

EN
L series

2025/847

7.5.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/847

of 6 May 2025

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ([1]), and in particular Article 5e(5) thereof,

Whereas:

(1) The European Digital Identity Framework ('framework') set out in Regulation (EU) No 910/2014 is a crucial component in the establishment of a secure and interoperable digital identity ecosystem across the Union. With the European Digital Identity Wallets ('wallets') as its cornerstone, the framework aims to facilitate access to services across Member States, while ensuring the protection of personal data and privacy.

(2) Regulations (EU) 2016/679 ([2]) and (EU) 2018/1725 ([3]) of the European Parliament and of the Council, and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council ([4]) apply to the personal data processing activities under this Regulation. The rules on the assessment and provision of information established under this Regulation are without prejudice to the obligation to notify personal data breaches to the competent supervisory authority where applicable under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, and to the obligation to communicate the personal data breaches to the data subjects where applicable under these Regulations.

(3) The Commission regularly assesses new technologies, practices, standards and technical specifications. To ensure the highest level of harmonisation among Member States for the development and certification of the wallets, the technical specifications set out in this Regulation rely on the work carried out under Commission Recommendation (EU) 2021/946 ([5]) and in particular the Architecture and Reference Framework which is part of it. In accordance with recital 75 of Regulation (EU) 2024/1183 of the European Parliament and of the Council ([6]), the Commission should review and, if necessary, update this Regulation, to keep it in line with global developments and the Architecture and Reference Framework, and to follow the best practices on the internal market.

([1]) OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications (OJ L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework (OJ L 210, 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) In the event of a security breach or a compromise of the wallet solutions or of the validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014, or of the electronic identification scheme under which the wallet solutions are provided, reactions to such security breaches and compromises need to follow in a fast, coordinated and secure manner across Member States to protect users and to maintain trust in the digital identity ecosystem. This is without prejudice to Directive (EU) 2022/2555 of the European Parliament and of the Council ([7]) and Regulations (EU) 2019/881 ([8]) and (EU) 2024/2847 ([9]) of the European Parliament and of the Council, in particular as regards handling of incidents or vulnerabilities and their consideration as security breaches. Therefore, Member States should ensure the timely suspension of the provision and the use of wallets affected by a security breach or compromise, or, where appropriate, their withdrawal.

(5) To ensure appropriate reactions to a security breach or compromise, Member States should assess whether a security breach or compromise of a wallet solution, of the validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014, or of the electronic identification scheme under which a wallet solution is provided, affects the reliability of that wallet solution or of other wallet solutions. Such an assessment should be based on uniform criteria, such as the number and category of wallet users, of natural persons, and of wallet-relying parties impacted, the nature of impacted data, the duration of the compromise or security breach, the limited availability of a service and financial losses, and the potential compromise of personal data. These criteria should provide Member States with flexibility and discretion to establish in a proportionate manner whether the reliability of a wallet solution is affected and whether the suspension or, where justified by the severity of the breach or compromise, the withdrawal of the wallet solution is appropriate. These criteria should not trigger an automatic withdrawal of a wallet solution or an automatic suspension of the provision and the use of a wallet solution, but they should be duly considered by Member States when deciding if a withdrawal, or suspension of the provision and the use, of a wallet solution are necessary.

(6) Due to the impact and inconvenience caused by suspending the use of wallet solutions, Member States will need to evaluate whether the revocation of wallet unit attestations or any other additional measures are necessary to react adequately to the security breach or compromise.

(7) To keep wallet users informed about the status of their wallets, they are to be provided with adequate information about security breaches or compromises affecting their wallets. As wallet-relying parties registered in the Union can also be affected by security breaches and compromises, relevant information on security breaches and compromises are also to be shared with them.

(8) To enhance transparency and build trust into the digital identity ecosystem, the information about the security breaches or compromises and about their consequences should at least include the information required under this Regulation. Information concerning security breaches or compromises shared to wallet users and wallet-relying parties should however be carefully assessed so that to prevent and minimise the risk of their exploitation by attackers.

([7]) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) To enable users to access their wallet units again after a security breach or compromise has been remedied, the Member State that provided the wallet solutions, will need to re-establish the provision and use of that wallet solutions without undue delay. This can be done by re-establishing the wallet units, by issuing wallet units provided under a new version of the wallet solutions or by re-issuing new valid wallet unit attestations. Wallet users affected, wallet-relying parties, single points of contact designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014 and the Commission are to be informed accordingly.

(10) To ensure the withdrawal of wallets where a security breach or compromise has not been remedied within three months of the suspension or where this is justified by the severity of the security breach or compromise, the Member State should ensure that the relevant wallet unit attestations are revoked and that they cannot revert to a valid state nor be issued or provided to existing wallet units. Moreover, no new wallet units should be provided under the affected wallet solution. For transparency purposes, users, relying parties, single points of contact designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014 and the Commission need to be informed of the withdrawal. This includes a description of the potential impacts on the wallet users and notably the management of issued attestations, or on wallet-relying parties.

(11) The period of three months following the suspension of the provision and the use of a wallet solution, and during which the security breach or compromise having led to that suspension is to be remedied, should provide for a time limit after which the wallet solution is to be withdrawn unless an appropriate remedy has been implemented. Member States however are free to require the security breach or compromise to be remedied within a time limit that is shorter than three months, taking into account, in particular and where relevant, the extent, duration and consequences of that security breach or compromise. Where the security breach or compromise is not or cannot be remedied within the time limit set by the Member State, the Member State may require the wallet solution to be withdrawn before the expiration of the period of three months. Member States should use this time period during which a security breach or compromise that led to the suspension of the provision and the use of a wallet solution has to be remedied to prepare the potential withdrawal of that wallet solution and the resulting communications.

(12) To reduce the administrative burden for Member States regarding the information to be provided, in accordance with this Regulation, to the Commission and to other Member States, Member States should use existing notification tools such as the Cyber Incident Reporting and Analysis System ('CIRAS') operated by the European Union Agency for Cybersecurity ('ENISA'). Regarding alternative channels or means to be utilised to inform wallet users affected by a security breach or compromise and wallet-relying parties, Member States should ensure that the relevant information is provided in a clear, comprehensive, and easily accessible manner. The channels to provide such information to wallet users affected and wallet-relying parties should include appropriate solutions for website-based broadcasting, real-time tracking of website updates and news aggregation.

(13) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered its opinion on 31 January 2025.

(14) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter

This Regulation lays down rules for reactions to security breaches of the wallets, of the validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014, and of the electronic identification scheme under which the wallets are provided.

Article 2

Definitions

For the purpose of this Regulation, the following definitions apply:

(1) 'wallet solution' means a combination of software, hardware, services, settings, and configurations, including wallet instances, one or more wallet secure cryptographic applications and one or more wallet secure cryptographic devices;

(2) 'wallet user' means a user who is in control of the wallet unit;

(3) 'wallet-relying party' means a relying party that intends to rely upon wallet units for the provision of public or private services by means of digital interaction;

(4) 'wallet instance' means the application installed and configured on a wallet user's device or environment, which is part of a wallet unit, and that the wallet user uses to interact with the wallet unit;

(5) 'wallet secure cryptographic application' means an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device;

(6) 'wallet secure cryptographic device' means a tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographic functions for the secure execution of critical operations;

(7) 'wallet provider' means a natural or legal person who provides wallet solutions;

(8) 'wallet unit' means a unique configuration of a wallet solution that includes wallet instances, wallet secure cryptographic applications and wallet secure cryptographic devices provided by a wallet provider to an individual wallet user;

(9) 'critical assets' means assets within or in relation to a wallet unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the wallet unit;

(10) 'wallet unit attestation' means a data object that describes the components of the wallet unit or allows authentication and validation of those components.

Article 3

Establishing a security breach or compromise

1. Without prejudice to Directive (EU) 2022/2555 and to Regulations (EU) 2019/881 and (EU) 2024/2847, Member States shall duly consider the criteria set out in the Annex I to this Regulation to assess whether a security breach or compromise of a wallet solution, of the validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014, or of the electronic identification scheme under which the wallet solution is provided, is affecting their reliability or the reliability of other wallet solutions.

2. Where a Member State establishes, on the basis of the assessment laid down in paragraph 1, that a security breach or compromise is affecting the reliability of a wallet solution and suspends the provision and the use of that wallet solution, that Member State shall take the measures set out in Articles 4 and 5. Where a Member State withdraws the wallet solution, that Member State shall take the measures set out in Articles 8 and 9.

3. Where a Member State becomes aware of information relating to a possible security breach or compromise possibly affecting the reliability of one or more wallet solutions provided by another Member State, that Member State shall, without undue delay, communicate to the Commission and the single points of contact of the affected Member States designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014 on that fact. This communication shall include the information set out in Article 5(2).

4. The Member State receiving information provided pursuant to paragraph 3 shall take the measures set out in paragraphs 1 and 2 without undue delay.

Article 4

Suspension of the provision and the use of wallets and other remedies

1. Member States shall ensure that no wallet units are provided, used or activated under the suspended wallet solution.

2. Member States shall evaluate whether revoking wallet unit attestations of the wallet units affected by the suspension of a wallet solution, or any other additional remedy, is necessary to react adequately to the security breach or compromise.

3. The measures set out in paragraphs 1 and 2 shall be taken without undue delay, and in any event no later than 24 hours after the suspension of the provision and the use of the wallet solution affected by the security breach or compromise.

4. The measures set out in paragraphs 1 and 2 shall not hinder affected wallet users from exercising their right to data portability set out in Article 5a(4), point (g) of Regulation (EU) No 910/2014. This is under the condition that this right may be exercised by wallet users without impairing the security of the critical assets of the affected wallet units, in particular considering the reasons for suspension and the need to ensure the effective protection of those assets against misuse.

Article 5

Information about suspensions and remedies

1. Information in a clear, comprehensive and easily accessible manner about the suspension of the provision and the use of a wallet solution shall be provided, without undue delay and no later than 24 hours after the suspension of the provision and the use of the wallet solution, to:

(a) the single points of contact designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014;

(b) the Commission;

(c) the wallet-users affected;

(d) the wallet-relying parties registered in accordance with Article 5b of Regulation (EU) No 910/2014.

2. The information provided in accordance with paragraph 1 shall include at least the following:

(a) the name of the provider of the wallet solution the provision and the use of which has been suspended;

(b) the name and reference identifier of that wallet solution, as indicated in the list of certified wallets drawn up pursuant to Article 5d of Regulation (EU) No 910/2014, and, where applicable, the concerned versions;

(c) the date and time when the security breach or compromise was detected;

(d) if known, the date and time when the security breach or compromise became effective, based on network or system logs or other data sources;

(e) the date and time of the suspension of the wallet solution;

(f) contact details, including at least an email address and a telephone number for the notifying Member State, and, where different, for the wallet provider referred to in point (a);

(g) a description of the security breach or compromise;

(h) a description of the data compromised, including, where applicable, the categories of personal data as defined in Article 9(1) and Article 10 of Regulation (EU) 2016/679;

(i) where possible, an estimate of the approximate number of wallet users affected and of other natural persons affected;

(j) a description of the potential impacts on wallet-relying parties or on wallet users, and in the latter case, where relevant, any indications of measures that wallet users can take to mitigate those potential impacts;

(k) a description of the measures taken or planned to remedy the security breach or compromise, together with a planning and deadline for such remedy;

(l) where applicable and appropriate, a description of the measures taken or planned for transitioning wallet users affected to alternative wallet solutions or services.

Article 6

Re-establishment of the provision and the use of wallets

Where necessary to ensure the re-establishment of the provision, the activation and the use of a wallet solution, Member States shall without undue delay:

(1) re-establish the provision and use of the wallet units provided under that wallet solution by issuing a wallet unit provided under a new version of the wallet solution to all affected users;

(2) issue new wallet unit attestations to new wallet units or, where applicable, to previously issued wallet units, provided those wallet units fulfil the security requirements in place after the security breach or compromise is remedied;

(3) repeal any measure implemented pursuant to Article 4 and hindering the provision of new wallet units under the affected wallet solution, where that measure was linked solely to the now remedied security breach or compromise.

Article 7

Information about re-establishment

Where a Member State re-establishes a wallet solution, that Member State shall ensure that:

(1) information about that fact is provided without undue delay to all parties having received information on the suspension of the provision and the use of that wallet solution in accordance with Article 5(1).

(2) information provided pursuant to point (1) shall include at least the elements referred to in Article 5(2), points (a), (b) and (f) to (h) and the following:

(a) the date and time when the security breach or compromise was remedied;

(b) the date and time of the re-establishment of the affected wallet solution, and, where appropriate, of the affected wallet units provided under that wallet solution;

(c) a description of the measures taken to remedy the security breach or compromise;

(d) a description of the potential residual impacts on wallet-relying parties or on wallet users, and in the latter case, where relevant, any indications of measures that wallet users can take to mitigate those potential residual impacts.

Article 8

Withdrawal of wallets

1. If a security breach or compromise having led to the suspension of the provision and the use of a wallet solution is not remedied within three months after the date of suspension of the provision and the use of that wallet solution, the Member State providing that wallet solution shall ensure the affected wallet solution is withdrawn and its validity is revoked, without undue delay and in any event within 72 hours after the period of three months has expired.

2. When a Member State withdraws a wallet solution, it shall ensure that:

(a) the wallet unit attestations of the wallet unit of the affected wallet solution are revoked;

(b) the wallet unit attestations cannot revert to a valid state;

(c) no new wallet unit attestation can be issued to existing wallet units provided under the affected wallet solution;

(d) no new wallet unit can be provided under the affected wallet solution.

3. The measures set out in paragraphs 1 and 2 shall not hinder affected wallet users from exercising their right to data portability set out in Article 5a(4) point (g) of Regulation (EU) No 910/2014. This is under the condition that this right may be exercised by wallet users without impairing the security of the critical assets of the affected wallet units, in particular considering the reasons for withdrawal and the need to ensure the effective protection of those assets against misuse.

Article 9

Information about withdrawal

1. Information in a clear, comprehensive and easily accessible manner about the withdrawal of a wallet solution shall be provided, without undue delay and no later than 24 hours after the withdrawal of the wallet solution, to:

(a) the single points of contact designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014;

(b) the Commission;

(c) the wallet users affected;

(d) the wallet-relying parties registered in accordance with Article 5b of Regulation (EU) No 910/2014.

2. Information provided in accordance with paragraph 1 shall include at least the following:

(a) the name of the provider of the wallet solution which has been withdrawn;

(b) the name and reference identifier of that wallet solution, as indicated on the list of certified wallets drawn up pursuant to Article 5d of Regulation (EU) No 910/2014, and, where applicable, the concerned versions;

(c) the date and time of the detection of the security breach or compromise that led to the withdrawal of the affected wallet solution because of its severity or because it was not remedied within three months;

(d) if known, the date and time when the security breach or compromise became effective, based on network or system logs or other data sources;

(e) the date and time of the withdrawal of the wallet solution and of the effective revocation of the wallet unit attestations of the wallet units provided under the wallet solution;

(f) whether the withdrawal is the result of the severity of the security breach or compromise or is the consequence of the security breach or compromise not being remedied;

(g) contact details, including at least an email address and a telephone number for the notifying Member State, and, where different, for the wallet provider referred to in point (a);

(h) a description of the security breach or compromise;

(i) a description of the data compromised, including, where applicable, the categories of personal data as specified in Article 9(1) and Article 10 of Regulation (EU) 2016/679;

(j) where possible, an estimate of the approximate number of wallet users affected and of other natural persons affected;

(k) a description of the potential impacts on wallet-relying parties or on wallet users, and in the latter case, where relevant, any indications of measures that wallet users can take to mitigate those potential impacts;

(l) a description of the measures taken or planned for transitioning wallet users affected to alternative wallet solutions or, where applicable and appropriate, alternative services.

Article 10

Information system

Member States shall send information set out in Articles 3, 5, 7 and 9 to the Commission and the single points of contact of the Member States designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014, via the CIRAS operated by ENISA, or an equivalent system agreed by the Member States and the Commission.

Article 11

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States, except for Article 10, which shall apply from 7 May 2026.

Done at Brussels, 6 May 2025.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

Criteria for the assessment of a security breach or compromise

1. Member States shall base their assessment of a security breach or compromise on the following criteria:

(a) the breach or compromise has caused or is capable of causing the death of a natural person or considerable damage to a natural person's health;

(b) a successful suspectedly malicious or unauthorised access to the network and information systems of a wallet provider, of provider of validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014, or of a provider of the electronic identification scheme under which a wallet solution is provided ('concerned entities') has occurred, or is capable of occurring, in a way that is capable of causing severe operational disruption, and those systems are critical components of the affected wallet solution, of the affected validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014 or of the affected electronic identification scheme under which a wallet solution is provided;

(c) a wallet solution, a validation mechanism referred to in Article 5a(8) of Regulation (EU) No 910/2014, or an electronic identification scheme under which a wallet solution is provided, or a part of them:

— is completely or projected to be completely unavailable to wallet users or wallet-relying parties for more than 12 consecutive hours;

— is unavailable or projected to be unavailable to wallet users or wallet-relying parties, for more than 16 hours calculated on a calendar week basis;

(d) it is suspected that more than 1 % of the wallet users or wallet-relying parties are impacted or are projected to be impacted by limited availability of the wallet solution, or of the services provided by concerned entities as regards the wallet solution;

(e) there is a capability of compromise or there has been a compromise of physical access restricted to trusted personnel of concerned entities, or of the protection of such physical access, to one or more of the locations of network and information systems supporting the wallet solution, the provision of the validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014 associated with a wallet solution, or the electronic identification scheme under which a wallet solution is provided;

(f) the privacy, integrity, confidentiality or authenticity of data stored, transmitted or processed in the wallet solution is compromised, or is capable of being compromised, in one or more of the following ways:

— it has an impact on more than 1 % of the wallet users of the affected wallet solution or on more than 100 000 of those wallet users, whichever number is smaller;

— it is a result of a successful suspectedly malicious activity;

— it is a result or is likely to be a result of one or more known vulnerabilities, including those handled in accordance with Commission Implementing Regulation (EU) 2024/2981 ([1]);

— it is likely to impact personal data in a manner that is likely to result in a risk to the rights and freedoms of the natural persons concerned and, in particular, in case of breach of personal data as defined in Articles 9(1) and 10 of Regulation (EU) 2016/679;

([1]) Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets (OJ L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— it is likely to impact personal electronic communications;

— it is likely to result in a high risk to the rights and freedoms of natural persons;

— it is likely to impact vulnerable natural persons;

(g) the certification of the wallet solution has been cancelled or is projected to be cancelled;

(h) the breach or compromise has caused or is capable of causing direct financial loss for a concerned entity, and that loss exceeds EUR 500 000 or, where applicable, 5 % of the concerned entity's total annual turnover in the preceding financial year, whichever is lower.

2. Member States shall not consider planned consequences of a maintenance operation carried out by or on behalf of the concerned entities, provided such maintenance operation:

(a) has been notified in advance to potentially affected wallet users, wallet-relying parties and relevant competent supervisory bodies;

(b) does not meet any of the criteria set out in paragraph 1 of this Annex.

3. As regards to point (c) of paragraph 1, the duration of an incident affecting availability shall be measured from the moment the proper provision of the affected service is disrupted until the moment the service is restored and operational again. Where a concerned entity is unable to determine the moment when the disruption began, the duration of the incident shall be measured from the moment the incident was detected, or from the moment when the incident was recorded in network or system logs or other data sources, whichever is earlier. Complete unavailability of a service shall be measured from the moment the service is fully unavailable to users, to the moment when regular activities or operations have been restored to the level of service provided prior to the incident. Where a concerned entity is unable to determine when the complete unavailability of a service began, the unavailability shall be measured from the moment it was detected by that entity.

4. As regards point (d) of paragraph 1, limited availability of a service is considered to occur in particular when a service is considerably slower than the average response time, or where not all functionalities of a service are available. Where possible, objective criteria based on the average response times of services shall be used to assess delays in response time.

5. To determine the direct financial losses resulting from a breach or compromise referred to in point (h) of paragraph 1, concerned entities shall take into account all financial losses incurred as a result of the incident, such as costs for replacement or relocation of software, hardware or infrastructure, staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills, fees due to non-compliance with contractual obligations, costs for redress and compensation to customers, losses due to forgone revenues, costs associated with internal and external communication, and advisory costs, including costs associated with legal counselling, forensic services and remediation services. Costs necessary for the day-to-day operation of the business, such as costs for general maintenance of infrastructure, equipment, hardware and software, improvements and risk assessment initiatives, and insurance premiums shall not be considered as financial losses resulting from an incident. The concerned entities shall calculate the amounts of financial losses based on available data and, where the actual amounts of financial losses cannot be determined, those entities shall estimate those amounts.