EUROPEAN
COMMISSION

Brussels, XXX
[…](2024) XXX draft

ANNEX 1

ANNEX

to the

Commission Implementing Regulation

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

ANNEX I

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 financial loss for a wallet provider, a provider of validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014, or a provider of the electronic identification scheme under which a wallet solution is provided ('relevant entities'), that exceeds500 000 EUR or, where applicable, 5 % of the relevant entity's total annual turnover in the preceding financial year, whichever is lower.

   (b) In order to determine the financial losses resulting from a breach or compromise, relevant 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, 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 relevant entities shall calculate the amounts of financial losses based on available data and, where the actual amounts of financial losses cannot be determined, the entities shall estimate those amounts.

   (c) 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.

   (d) A successful suspectedly malicious or unauthorised access to network and information systems of a relevant entity, which 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, occurred.

   (e) 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 for more than 12 consecutive hours; or

      – is unavailable to wallet users or wallet-relying parties, for more than 16 hours calculated on a calendar week basis.

      – The duration of an incident which impacts availability, shall be measured from the time of disruption of the proper provision of the affected service until the time of recovery. Where a relevant 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 that was provided prior to the incident. Where a relevant 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.

(f) Suspectedly 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 relevant entities as regards the wallet solution.

(g) Limited availability of a service is considered to occur in particular when a service is considerably slower than 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. Complete unavailability of a service shall be measured from the moment the service is fully unavailable to wallet users or wallet-relying parties, to the moment when regular activities or operations have been restored to the level of service that was provided prior to the incident. Where a relevant 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.

(h) Physical access to one or more of the areas where 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 to a wallet solution, or the electronic identification scheme under which a wallet solution is provided, are located and to which access is restricted to trusted personnel of relevant entities, or the protection of such physical access, is compromised.

(i) The privacy, integrity, confidentiality or authenticity of data stored, transmitted or processed in the wallet solution is compromised in one or more of the following manners:

(j) 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 likely to affect personal data as defined in Articles 9(1) and 10 of Regulation (EU) 2016/679;
- it is likely to affect personal electronic communications;
- it is likely to result in a high risk to the rights and freedoms of natural persons;
- it is likely to affect vulnerable individuals.

(k) The certification of the wallet solution was cancelled.

(l) The breach or compromise has occurred at least twice within six months with the same apparent root cause and the collective occurrences meet any of the criteria set out in the other points of paragraph 1 of this Annex.

2. Planned consequences of a maintenance operation carried out by or on behalf of the relevant entities shall not be considered, 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.