

ANNEX II

REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
 - (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
 - (b) the electronic signature creation data used for electronic signature creation can practically occur only once;
 - (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
 - (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.
2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.
3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.
4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:
 - (a) the security of the duplicated datasets must be at the same level as for the original datasets;
 - (b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

Changes to legislation:

There are currently no known outstanding effects for the Regulation (EU) No 910/2014 of the European Parliament and of the Council, ANNEX II.