Brussels, 13 March 2013

Vice-President Neelie Kroes
Commissioner for Digital Agenda
European Commission
B – 1049 Brussels

Dear Vice-President Kroes,

On behalf of the Article 29 Working Party I would like to share with you some remarks and concerns that emerged in the course of a first analysis of the **Commission's proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market** from a data protection point of view.

This letter will first make some general remarks regarding the used terminology in the proposal (1). Next, some comments will be made on the content of the proposal, starting with electronic trust services (2), followed by remarks on electronic identity (3). Finally, the matter of security and trust will be discussed (4).

1. General Remarks

Terms and definitions

Some terms used in the Regulation proposal have a different meaning compared to their denotation in relevant international standards and in the Identity Management Community. Some examples will be mentioned below.

Authentication

Authentication is defined in the proposal as "an electronic process that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data". This definition takes no notice of authentication systems that allow the validation of an electronic credential which is not an electronic identification.

Identity

Another example of the use of a term in the proposal that is not in line with the definition that is commonly used is ‘identity’. “Identity” is defined e.g. in ISO/IEC 24760-1 as a “set of attributes related to an entity”. The proposal however defines “identity” also as being “unambiguous”. Article 3 (1) states that: ”‘electronic identification’ means the process of using person identification data in electronic form unambiguously representing a natural or legal person”.

It may be more useful to prefer more general definitions in line with international practice to avoid confusion. The Article 29 Working Party has for example provided definitions of authentication and identification in its Opinion WP 80/2003 that could serve as a model.

“Unambiguous identity”

In different articles the proposal requires identification data or identifier to be “unambiguous”, for example in Articles 3 (1), 6 (1) c or 7 (1) c. It is not clear whether or not the Regulation admits privacy by design models that aim at enhancing data protection by avoiding the use of unambiguous identifiers. It is important that the Regulation will be clear about what is meant with ‘unambiguous identity’ for several reasons.

Firstly, it is important to note that “unambiguous person identifiers” do not exist in all EU member States for legal or constitutional reasons. In some countries sector specific identifiers are used. In other countries there are national identifiers that can only be used for specific purposes and/or may not be disclosed. Examples: In Lithuania a qualified trust service provider included the national identifier in the certificate of eSignatures. This has been prohibited by the DPA and the Supreme administrative court because there is no legal basis for using this identifier in the certificate and because the use of this identifier in the certificate would have resulted into making this identifier public. In Austria there is no single national identifier but a system of sector specific identifiers.

Secondly, while the disclosure of the signatory’s full identity may be required in some use-cases, there are many circumstances in which a disclosure of the whole set of available data is not required (e.g. age verification and citizenship verification) and in some situations even a pseudonym would be sufficient. Considering the data protection principle of data

minimization, systems requiring only the minimum of information to fulfil the given purposes should not only be recognised and accepted, but rather mandated by the Regulation.

Examples:

- As already used in some EU member States, sector-specific eID systems aim at enhancing data protection by using sector specific (and thus non-unique) identifiers (for entities in different sectors). Only the relying parties within the same sector are able to validate those eIDs.
- New systems of authentication allow users to prove some attributes (like being over 18, or being a subscriber to a given online journal) or even to prove some attribute value assertion (like being over 12 and below 25) to obtain a special feature.
- New privacy preserving signatures, like group signatures allow a user to sign a document as a member of a group. In this case the signatory is not identifiable by public verification of the signature. If needed, only a specific authority is able to identify that user.

In other words: in some applications revealing the unambiguous identity of an individual is not necessary at all. The Regulation should therefore encourage the use of technologies and/or organisational rules that support and enhance data minimization.

Pseudonyms

One of the solutions to protect privacy while using eID systems is to use pseudonyms. While pseudonyms are mentioned in the eSignature parts of the Regulation, they are not mentioned in the other parts. It may be worth to consider to explicitly allowing the use of pseudonyms in the other parts as well to promote this privacy friendly instrument.

Pseudonyms can be created in multiple ways. They may be chosen by the users themselves (for example “artist names”), be created randomly or be defined by the system in order to provide the user with a different pseudonym for different services, in a similar way as the German eID attributes. The design of these systems is more privacy friendly as the same unique identifiers are not used in all data processing operations. Pseudonyms should therefore be mentioned in the general part of the Regulation in order to avoid giving the impression that the use of pseudonyms is limited only to eSignatures.

Personal data included in certificates

Under Art. 11(3) of the draft Regulation trust service providers are required to guarantee the confidentiality and integrity of data related to a person to whom the trust service is provided. Annex 1 presents a set of information requirements to be included in a qualified certificate for eSignatures. These are data from the service providers issuing the certificate and signatories for which the certificate is issued. The required information is at least the name or a pseudonym and other data which unambiguously identify the certificate holder. It is not excluded that this set of information will include personal data of the certificate holder which are not necessary for the document recipient in the verification process. The draft Regulation does not consider this issue at all, except for mentioning in Art. 11 (2) that processing shall be strictly limited to the minimum data needed to issue and maintain a certificate or to provide a trust service. However, the text of the Regulation does not properly take into account that this necessary minimum data set to ensure trust can be different depending on who is the recipient of the information. In the relationship between the certificate holder and the service provider issuing the certificate the required minimum of personal data will usually be different compared to what is required in the relationship between the certificate holder and the person verifying an electronically signed document.

Example:
Company X employs Mr Y as Trade Department Director and buys him a certificate for signing contracts concluded on behalf of Company X. The certificate identifying Mr Y includes information on his name, position at Company X and additional data unambiguously identifying Mr Y. For a customer of Company X during the verification of a document signed by Mr Y it is only necessary to verify that the document was signed by a person Y representing X. There is no need to know the data unambiguously identifying Mr Y as a natural person like his birth date or his private address. The latter data are necessary for the service provider issuing the certificate or for the employer, but they are not necessary for entities verifying the signed document. The data which are not necessary (here, e.g. Mr Y's home address) shall not be disclosed to the other parties that do not need those data.

Directive 95/46/EC applicability

Art.11 only mentions trust service providers but not eID providers. Directive 95/46/EC applies to all processing of personal data, therefore if a reference is made in the Regulation; it should include all service providers and not only one of them.

The wording of Art.11 (3) which makes reference only to the confidentiality and integrity of the data related to the person to whom the service is provided raises some concerns about other principles of data quality and data security like availability, authenticity, accuracy, non-linkability and intervenability that are not mentioned. This could create the impression that these objectives must not be observed.

Finally, as already mentioned above, the implementation of the key concept of data minimization is not being emphasized enough in the Regulation proposal. There are many use-cases where the whole set of available personal data is not required to use the service provided (e.g. age verification) and in some use-cases even a pseudonym would be sufficient but the proposal does not take this issue into consideration.

2. Remarks on electronic trust services (Article 3 and 20-27)

Seal and mass signatures

The currently sometimes problematic need to sign with "qualified (personal) signatures" documents (receipts) en masse seems to be addressed by the proposal through the introduction of the "seal" (Article 28). This seal seems not to be linked to an individual but to the creator – which according to Art 3 (19) must be a legal person. While the Regulation specifies these requirements it does not specify what the intended purposes are. The purposes of seals are only mentioned in the Recitals 42, 43 and 47. They should also be specified in a substantive provision.

Finally if the intention was to cover the "mass receipt" phenomena, this newly introduced instrument would still leave out businesses without legal personality (e.g. one person companies or the German KG (Kommanditgesellschaft) or OHG (offene Handelsgesellschaft).

Qualified signature for employees

In order to promote the use of electronic signatures several data protection authorities have reported that employers buy and activate electronic signatures for their employees. While common sense would imply that only the signatory should be able to activate a qualified electronic signature, even if he has not bought that service, this is not always respected by employers. The current proposal does not specifically address this known issue.

3. Remarks on electronic Identity

As stated in the general remarks, the Directive 95/46/EC shall be considered in the entire Regulation. In particular, we express serious concerns about the absence of references to the Directive in the electronic identification chapter because electronic identification is a domain where data protection must be taken into account.

Principle of data minimization

We consider it to be essential to preserve and promote privacy friendly systems introduced at national level, especially when they implement the principle of data minimisation. For example, the German eID contains a set of attributes such as age, name, nationality etc… that can be individually disclosed. The system requires the service provider to prove that he needs a particular attribute for the specific service. The principle of data minimization requires that third party services may not ask for more than the necessary information. As not all the set of attributes relating to the user will be needed every time they should not be disclosed systematically to identify that user and/or authenticate a document signed by that user. This solution is therefore in accordance with the Directive 95/46/EC, especially with regard to the principle of minimization of personal data and thus should be preserved and promoted.

Furthermore, the current proposal does not consider more privacy friendly technology such as the more advanced cryptographic solutions allowing only needed information (for example nationality) to be decrypted and disclosed without revealing the whole identity. This is prevented by article 6 (d) which states that EU member States shall not impose any specific technical requirement on relying parties established outside of their territory intending to carry out authentication. Conversely, privacy friendly systems such as the cryptographic solution mentioned above will most likely require the use of additional software. We believe that article 6 (d) needs address that issue. If MSs shall not impose any technical requirement to the other MSs, nevertheless certain requirements may and must be specified in the context of the Coordination requirements pursuant to Art. 8 where certain technical standards may be agreed upon and enforced through implementing acts.

Danger of profiling through online authentication and validation systems

Trust service providers know their clients precisely and also get information on which online services their clients use through the identification, authentication and validation processes. While this might appear adequate for ensuring the availability of the service and necessary to

minimize potential liability, such processing should however not lead to the creation of a profile of an individuals' behaviour. That is in conflict with existing and upcoming European privacy legislation. Rules that regulate the collection, the use and the deletion of these data should be laid down in the Regulation in order to ensure more consistency and legal certainty.

4. Remarks on security and Trust (Article 15-19)

Security of electronic signatures

While formal aspects of cooperation, recognition, supervision and the establishment of trusted services are regulated in the proposal, fundamental data security requirements are not set forth. In Article 15, the proposal refers to the state of the art measures that must be taken to manage the risk posed to the security of the trust service. While this flexible legal reference to the best industrial standards can be helpful when it comes to auditing a service or a device, it is not very meaningful when it comes to judging the organisational aspects of handling that technology. It must be remembered that data security can not only be achieved through technical measures but always requires adequate organisational and behavioural rules.

For example, it is currently lawful in some Member States to cache an electronic signature in order to make it easier to sign invoices and similar documents en masse. Through such an implementation of the current eSignature Directive (1999/93/EC) – which also leaves the question open about the conditions and limits under which an individual must create electronic signatures – in these countries even a deceased person is still able to sign with a qualified electronic signature until the time limit of the caching mechanism has been reached. The strong legal effects of a handwritten signature are based on the fact that it must be performed in person and can only be performed in limited amounts due to physical limits. If the same legal effects are granted to an electronic signature the same safeguards need to apply.

The data protection principle of accuracy should be addressed in this context with clear definitions of certain minimum technical and organisational measures that shall be taken to ensure that electronic signatures are always generated with the signers' cooperation. Article 15 (5) empowers the Commission to further specify security measures in delegated acts, but there is no obligatory mandate. Indeed Recital 51 of the proposal indicates that "implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards which use would give a presumption of compliance with certain

requirements laid down in this Regulation or defined in delegated acts". Nevertheless the proposal does not explicitly mention for what provisions this should be done.

Supervisory authorities

The proposal mentions “Independent body”, “supervisory body” and “data protection authorities” in articles 16 and 15 (2).

It is not clear if those terms describe the same body and/or whether this refers to the already existing data protection authorities or other existing bodies or intends to introduce new supervisory bodies. All three mentioned bodies are in charge of auditing the trust service provider. While it may be useful to double-check in specific circumstances, it should be specified and clarified which role has to be played by each of those bodies unless the proposal only describes one body using different terms. In that process the different tasks of the bodies mentioned in other regulations/directives (e.g. Art.4 of the ePrivacy Directive, Art.31, 32 of the data protection draft Regulation) need to be considered. Consistency has to be ensured.

List of qualified trust services

The article 17 describes the procedure needed for a trusted service to obtain a qualification. It seems hard to understand how a service provider may provide qualified trusted services before he is fully accredited by the supervisory body and included as such in the trusted list. To include not yet qualified services on that list may undermine the global level of trust in that list because “trust” only comes from being referenced as “qualified trust service provider” in that list. Electronic systems would not only have to check if an entity is on that list but would also have to check if there are any restrictions or not. Including not qualified trust service providers on the “qualified trust service providers list” is confusing and a source of error. This seems not to be in line with the general data protection principle of accuracy.

Security Level definition

The proposed Regulation does not establish any minimum security level. Minimum requirements regarding data security and relevant standards should be laid down in primary legislation itself and not only in delegated acts. As different services need different levels of security, such levels of security should be defined. For example, the STORK project, which deals with the interoperability of the eID systems in the EU, acknowledges 4 distinct levels to deal with the different security requirements needed in different use cases. In a more general way, the Common Criteria standard (ISO/IEC 15408) defines 7 levels of evaluation

depending on the purposes of the system and the threats that it faces. It should be further noted that the SOGIS Mutual Recognition Agreement, based on an EU Council Decision, already builds a successful framework for coordinated security evaluation in Europe in this Common Criteria context. As an example, the SOGIS framework is used in the area of EU regulated tachygraphy.

The lack of general definitions of these levels may lead to a "race to the bottom" in terms of data protection and security. It would be therefore worthwhile to define minimum requirements on data security in the Regulation itself. The delegated acts could then define technical specifications for interoperability and security levels, based on the minimum security requirements set forth in the Regulation.

STORK project

Finally in its letter to the STORK partners from April 15 2011, enclosed with this letter, the Working Party 29 addressed several data protection relevant issues on the implementation of EU interoperable systems for recognition of electronic identities and authentication asking for similar safeguards and common standards. The points raised in the letter concerning the STORK experience are not addressed by the current proposal.

While it is understood that a Regulation should stay technically neutral and be open for future improvements, it should also set a common minimum standard on data protection and security and ideally solve all currently known issues in order to enhance trust in the system.

The Working Party will continue to closely monitor the developments regarding the Regulation.

Yours sincerely,

For the Working Party

The Chairman
Jacob KOHNSTAMM