

SANTE/2017/B2/027

**Expert revision of the Draft Interim Report III from the
Implementation Study on traceability and security features
in the field of tobacco products**

FINAL REPORT – 15 JULY 2017



1. Deliverables and meetings

The Model Contract drafted by Everis was provided by the DG SANTE to the external expert on 28 June 2017.

A first set of comments was communicated by the external expert to the DG SANTE on 4 July 2017 (see annex 1 attached).

The first meeting with the DG SANTE, Everis, and the external expert took place on 4 July 2017. Main comments were discussed and explained to Everis.

Everis provided a new version of the Model Contract on 11 July 2017. This version included various modifications made in order to address the comments made by the external expert (not all of them however – notably the definitions and the SLA).

Additional comments were communicated by the external expert to the DG SANTE on 12 July 2017 (see annex 2 attached), and discussed with DG SANTE and Everis during the meeting held on 12 July 2017 at the Commission's premises.

The purpose of this final report is to present the concluding remarks and some general comments on the Model Contract, as provided to the DG SANTE by Everis.

2. General remarks about the Model Contract

2.1. *Classical Data Storage Agreement*

A data storage contract is an agreement pretty usual in the IT Law practice (notably in the context of cloud computing). From a legal perspective, most clauses are similar and related to :

- Definitions;
- Scope and object (with references to technical annexes, including SLA);
- Main duties of the provider and the client;
- Acceptance of the deliverables (if applicable);
- Modification of the Services (change request);
- Price and invoicing (with references to annexes);
- Data Protection;
- Confidentiality;
- Intellectual property rights;
- Liability (or, more precisely, limitation of liability);
- Audit;
- Duration and termination;

- Effect of termination (including exit plan);
- Business continuity plan;
- Varia (Jurisdiction ; escalation process in case of dispute ; applicable law ; etc.)

Depending on the bargaining position of the Parties, the clauses will be more or less balanced, to the benefit of the provider or the client. In most cases, the clauses are drafted by the provider with low margin of negotiation of the client and the main risks therefore rely on the client.

Such kind of agreement shall include both legal and technical requirements to be respected by the provider.

Various projects were implemented at the EU level in the context of Cloud and we recommend to take them into account when determining the main rights and duties of the parties¹, notably from a technical point of view.

2.2. *Specific features of the present Data Storage Agreement*

In the present case, the Model Contract must be compliant with the requirements prescribed by the Tobacco Products Directive, as mainly referred to in Article 15 (8) – 15 (10) of the Directive :

- The Provider shall be independent from manufacturers and importers of tobacco products;
- The Provider shall have specific technical capacities;
- The data storage facility shall be physically located on the territory of the Union;
- Data storage contracts shall be approved by the Commission;
- Providers' activities shall be monitored by an external auditor;
- Access to the data storage facilities shall be given to the Commission, the competent authorities of the Member States and the external experts;
- Access to data could also be given to manufacturers and importers by the Commission or the Member States in duly justified cases;
- Recorded Data shall not be modified or deleted by an economic operator involved in the trade of tobacco products;
- Applicable data protection requirements (whether prescribed by the directive 95/46/EC or the General Data Protection Regulation) shall be respected.

¹ Please see for instance the documents available on <https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-service-level-agreements> (including, among others, Cloud Service level Agreement Standardisation Guidelines and a Code of Conduct for Cloud Services Providers). See also, with regard to data protection duties, Article 29 WP, "Opinion 2/2015 on C-SIG Code of Conduct on Cloud Computing", 22 September 2015 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf) or Article 29 WP, "Opinion 2/2012 on Cloud Computing", 1 July 2012 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf).

As a result, the Model Contract cannot be a copy/paste of all and any standard clauses usually found in a data storage agreement, where all rights on the data belong to the client. The provider must indeed play the role of a “trust service provider” (archiving provider), that must be independent from the client and cannot modify or delete the data upon request of economic operators involved in the trade of tobacco products.

Archiving services are not regulated at the EU level but other trust services are so, in the regulation EU 910/2014 on electronic identification and trust services (eIDAS Regulation). In some Member States, specific legal provisions were enacted in order to regulate the activities of archiving services providers². I therefore recommend to rely on the main principles applicable to the trust service providers, while determining the main rights and duties applicable to the data storage provider in the present case.

3. Focus on some legal key points to be included in the Model Contract

Various comments and suggestions were already included in the second version of the Model Contract provided by Everis.

The present section is therefore not exhaustive but summarize the main key points to be taken into account.

- Structure : as simple as possible, with the GTC, the technical annexes (including SLA) and a Work Order / Order Form.
- Definitions : key terms must be defined.
- Scope and object : main Services governed by the Agreement must be presented. In the present case, I understand that these Services relate to the (i) Data Storage ; (ii) Support and Maintenance and (iii) Access to the Data. It should be clearly explained and detailed, with functional requirements to be achieved. References must also be made to annexes, including SLA and documentation.
- Main duties of the Provider : references shall be made to its independence and technical capacities, as well as to all and any other specific requirements imposed by the Directive (in particular, the prohibition to delete or modify data or the place where data are stored) or in line with the duties of a Trust Service Provider.

² In Belgium, see for instance the Act of 21 July 2016 *mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique*. Please let me know, would you like to receive the relevant provision of this Act.

- Modification of the Services : this point must be included, taking into account the duty to get the approval from the Commission on the data storage contract.
- Data Protection : normally, the provider is considered as data processor and the client as the data controller, in the meaning of the applicable Data Protection Law, with the corresponding requirements to be complied with (in particular, Article 28 of the GDPR). One could however consider that the prohibition to delete or modify data is not consistent with the qualification of the client as “data controller”, as well as the access to data only provided by the Commission or the Member States in duly justified cases. The qualification of the activities of the Commission and the competent authorities of the Member States could therefore be discussed (joint data controllers?). This issue is pretty complex and the final option promoted by Everis should be adequately documented and justified.
- Confidentiality : most data shall be considered as confidential and/or subject to business secrecy. As a result, a confidentiality provision must be included in the Agreement. Please note however that a standard confidentiality clause cannot just be copied/pasted in the Model Contract, as some specific features applicable in the present case must be taken into account (in particular, the prohibition to delete or modify data or the access right granted to the Commission and the competent authorities).
- Right on Data (and ownership?), including access rights : the topic of the rights on the data is probably the most complex issue to be addressed in the Model Contract. It is indeed governed by distinct relevant applicable framework (Data Protection Law, IP Rights and specific duties, such like Art. 15 of the Directive), with corresponding requirements. The rights and duties of all parties must be explained and detailed in the Agreement. The solution promoted by Everis must also be adequately justified.
- Audit : main rules applicable to the audit must be defined in the GTC, as well as the consequences of an audit showing non-compliance of the provider’s activities with the Agreement or the legal framework (in particular, the Directive).
- Liability (or, more precisely, limitation of liability): limitations of liability are usual in data storage agreements (mainly with the exclusion of indirect damages or the introduction of liability cap, corresponding to the insurances of the provider). The solution proposed in the Agreement must be balanced (in particular, no limitation of liability for willful misconduct, gross negligence or violation of substantial duties, regulated in Data Protection or Confidentiality Clauses) and in line with the market practices (otherwise, there will not be any provider accepting to provide the Services at these conditions).
- Duration and termination : duration and termination clause should be drafted keeping in mind the purpose of stability of the Agreement. As a result, we recommend a

definite duration of 3-5 years (with tacit renewal) and the prohibition, for the provider, to terminate the Agreement for convenience. Termination for cause (clearly defined) should only be allowed. Possible insolvency of the provider could also give rise to the termination of the Agreement. In any cases, the Commission should be informed about such termination (and its grounds).

- Effect of termination (including exit plan) : this point is very important and must be regulated by the Model Contract, with technical details provided in a specific Annex (Exit Plan), stating the main duties of the Parties, the fees, the timeline, the format of data, the collaboration duties, etc.
- Business continuity Plan : main duties of the parties should be included in the GTC, with additional details in a relevant technical annex. It is particularly important in the present context.

4. Global appreciation of the Model Contract proposed by Everis

The quality of the first version of the Model Contract provided by Everis was pretty low, and various clauses, however usual in this kind of agreement, were missing.

The second version was better, although not yet sufficient. Some clauses are still missing (SLA, definitions, final of clauses on access right and data protection, no liability of the provider on the content stored, should it be illicit, etc.) and, therefore, could not be reviewed. Furthermore, some standard clauses introduced in the second version are obviously copied/pasted from standard IT contracts without the necessary amendments, aiming at complying with the requirements of the Directive. Attention must indeed be paid to the specific features of the agreement to be concluded, due to the complex applicable legal framework.

Some issues are pretty difficult to address (in the context of Data Protection or with regards to the rights on the data, including the access rights). Some choices must however be made in this context by Everis (e.g. qualification as data controller or processor pursuant to the GDPR). The stakeholders should however be able to understand the background and purposes of the promoted solutions and, for that reason, we recommend that their legal justification is explained and detailed by Everis in its report.