EMTOC Instruction for the electronic reporting of tobacco product ingredients via the Electronic Model TObacco Control (EMTOC) system

EMTOC Instruction version 1.2 February 2010

Preamble

This EMTOC Instruction is to be converted into the appropriate QM/QA document format used by the competent regulatory authorities of the Member States and can be translated for this purpose if necessary. In the absence of a QM/QA system, the EMTOC Instruction is to be formally recognised as an implicit part of the EMTOC Terms of Use. The EMTOC Terms of Use must be duly signed and sent by the all USERS. To apply for access to EMTOC, Reporting parties send the duly signed EMTOC Terms of Use to the REGULATOR of each member state, where information will be submitted. After approval by the local REGULATOR, access to EMTOC is granted by the Trust Centre. Regulators, who use EMTOC, send the duly signed EMTOC User Agreement directly to the Trust Centre.

Contents

1 Purpose

This Instruction regulates the procedure for electronic reporting on tobacco product ingredients in the Member States of the European Community. In particular, it regulates the management of the channel for secure transmission via the EMTOC system. Compliance with this Instruction is an element of the security strategy and is indispensable for ensuring data security.

This Instruction is designed to protect secret information on tobacco product formulation during the ingredient reporting process. It covers the period from submission of information via the EMTOC online portal, through transmission and storage in a database, up to the time of deletion from the system.
It is to be noted that the disclosure of sensitive details of the formulation for a tobacco product can cause considerable commercial damage to a company.

Essentially, the requirements of the REGULATOR'S IT security strategy are applicable with regard to data security and the management of sensitive electronic information. REGULATORS are requested to ensure that national specific rules on the protection of trade secret information are applied. This Instruction is to be understood as a supplement to REGULATORS' indispensable existing provisions concerning data security in relation to specific requirements associated with the submission of information on tobacco product ingredients.

The explanations of this Instruction and attached documents are applicable in Switzerland in the same way as for the Member States of the European Union except for the submission of data to the EC or data access and analysis by the EC, which is not intended.

2 Legal basis

In Directive 2001/37/EC, requirements for reporting tobacco product ingredients were introduced by the EU. This stipulates that every tobacco MANUFACTURER or IMPORTER is required to report to the competent regulatory authority on the ingredients contained in the products intended for distribution in the Member State in question.

The EU directive has been transposed into Member States' national law. Therefore reporting requirements within a Member State are based on national legislation, and reports are to be submitted to the authority specified therein (REGULATOR).

The European Commission's Practical Guide on "Reporting on tobacco product ingredients", issued on 31 May 2007, specifies the reporting format, which is the basis for the EMTOC system. Additionally required information is collected solely for the purposes of data processing and communication. In Switzerland the respective EC regulations are stipulated in the tobacco ordinance (SR 817.06, article 10).

3 Scope

This Instruction is applicable to all USERS of the electronic reporting system. This implies that it applies to parties registered for reporting on tobacco product ingredients and to those responsible for managing, updating, evaluating, forwarding or performing other authorised operations on the data.
The application of this Instruction requires the existence of an IT security strategy that functions to ensure the safety and security of ingredient data and hardware.

4 Terms/abbreviations

APPROVED THIRD PARTY	Regulators may decide to delegate their responsibilities in the verification and assessment of the data to an authorised third party. Staff members of this approved third party have to accept the User Agreement in the same way as the other USERS. They will get access to the data with the role "REGULATOR".
EC	European Commission. DG SANCO C6, Brussels
EMTOC	Electronic Model Tobacco Control (EMTOC): an electronic system set up to accommodate the issuance of the (mandatory) reports on tobacco product ingredients to the competent Regulator. EMTOC comprises a number of components facilitating simple, accurate and secure electronic transmission of Data and is accessible for Users via an online portal.
FOLDER	In the context of the Instruction, this is a defined storage area, generally corresponding to a directory on a server or a table in a database. For each folder containing CONFIDENTIAL INFORMATION, access rights are individually managed by the administrator.
IMPORTER	Natural or legal person responsible for importing a tobacco product from a third country to a Member State of the European Union and domiciled in a Member State of the EU.
INFORMATION	Within the context of the Instruction, this term covers all information transmitted in the course of confidential data exchange, e.g. sensitive documents, passwords and communications from the REGULATOR or the TRUST CENTRE.
IT	Information technology/management: department, group or people responsible for ensuring functionality.
Local storage device	Device used for storing electronic data, which may be portable or located at the USER'S workplace. Such devices include portable hard disks, desktop hard disks, USB sticks, other memory cards, diskettes, CDs/DVDs, mobile phones, PDAs, etc.
MANUFACTURER	Natural or legal person manufacturing tobacco products.
REGULATOR	The governmental body or institution which is, by virtue of the relevant national implementing directive 2001-37-EC, designated to supervise on the reporting on tobacco product ingredients and receive, archive and process the reports.
REPORTING PARTY	Any Importer or Manufacturer that is subject to the statutory

	reporting obligations pursuant to the (laws implementing into national legislation) EC directive 2001-37 and/or officers or legal entities to whom such Importer or Manufacturer has assigned its reporting obligations.
REPORTING PERIOD	The calendar year for which reports are to be submitted. The deadlines and submission periods are specified by the REGULATOR of each member state.
CONFIDENTIAL INFORMATION	All information which is (i) classified as confidential and /or (ii) for which the confidential nature is apparent from its content. For the avoidance of doubt, all Data processed through the EMTOC System, except for the general public in accordance with Table 3 of the European Commission's Practical Guide on 'Reporting on tobacco product ingredients', shall be considered Confidential Information. Confidential INFORMATION may comprise trade secrets as well as confidential toxicological data. Additional to the requirements of handling CONFIDENTIAL INFORMATION in the context of this Instruction the regulations about personal data protection have to be respected.
SMART CARD	Chip card in accordance with ISO 7816, ID-1 (85.60 × 53.98 mm), contains the user ID and the SSL key for secure transmission via https. The card has to be used with a card reader equipped with keypad and display for secure PC-independent USER identification, to allow the USER access to the EMTOC system.
TRUST CENTRE	The party that has been appointed by the member states that participate in the EMTOC project to manage the EMTOC system (*inter alia* responsible for the issuance of certificates and login data (user ID and passwords), the management of User accounts, and helpdesk services).
USER	Natural person for whom an application to be granted access to the EMTOC system for a Reporting Party, a Regulator or the European Commission was filed and accepted by the Trust Centre. Natural person authorised to use the system in a role listed under Section 6. Authorisation is granted exclusively to a specific person and must not be transferred to another person. Only REPORTING PARTIES are allowed in own responsibility to share one USER access and SMART CARD between authorised persons (responsible person and his deputy).

5 Principle

In general, the contact point for the REPORTING PARTY is the REGULATOR in the Member State in which reporting is to be performed. In emergency cases, the TRUST CENTRE is additionally to be contacted for the purpose of quick blocking of accounts. INFORMATION transmitted to the EMTOC system or acknowledgements received from the system are to be understood as reports to or from the REGULATOR.

INFORMATION is to be transmitted exclusively in the specified format by electronic means. To assist reporting parties in producing these formats, the REGULATOR provides an online form for direct entry of the required data.

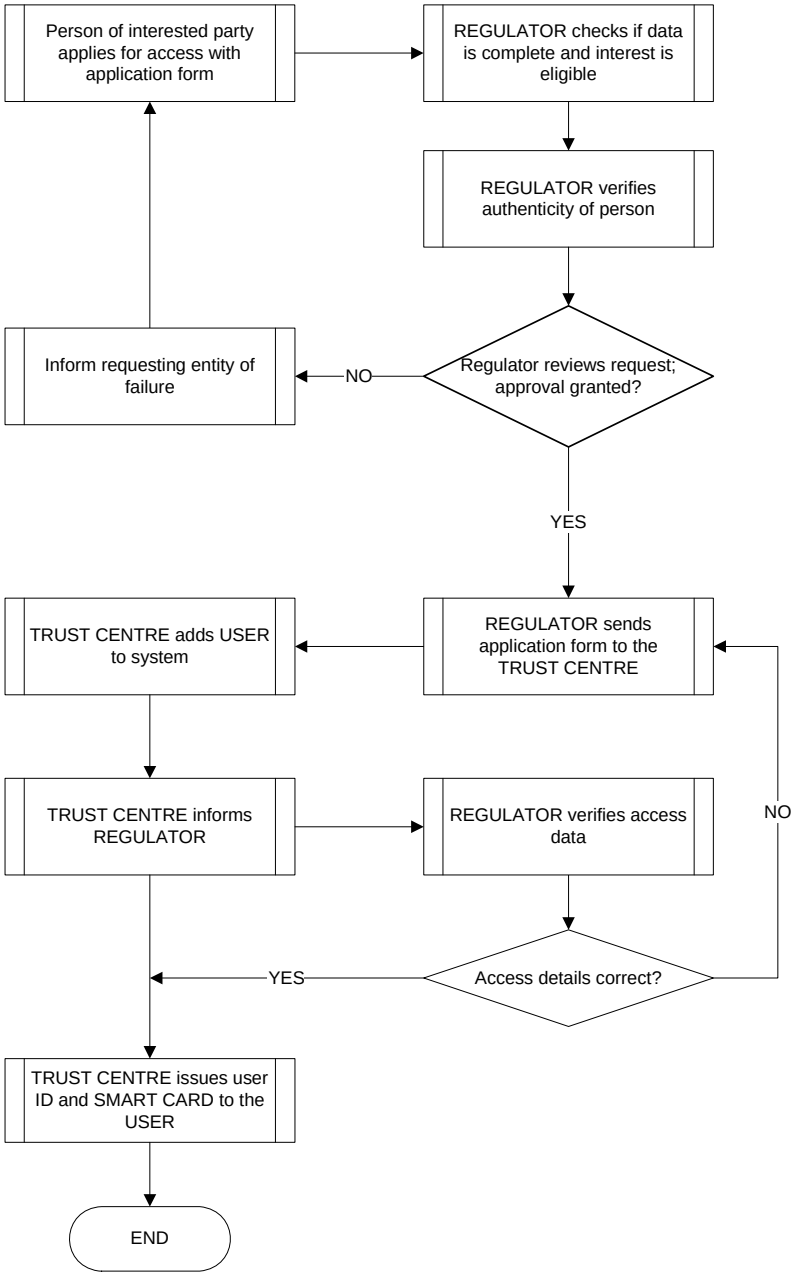
5.1 Granting of access

Access is requested by the USER and granted by the REGULATOR as follows:

1. Request for access by a REPORTING PARTY. The request is made through the management or authorised representative of the REPORTING PARTY, using an application form specifying the person responsible. The Terms of Use, application form and the User Agreement, is available online [LINK RIVM] in English (provision of the document in the national language by the REGULATOR is optional), are to be printed out, signed, sealed and sent to the REGULATOR.
2. The REGULATOR checks the USER'S identity, that the INFORMATION provided is correct, and the proposed use legitimate. The REGULATOR also checks that the USER has accepted the terms and conditions of use.
3. The REGULATOR requests the TRUST CENTRE to create a user profile, passing on the application form and indicating the USER'S role in accordance with Section 6.
4. The TRUST CENTRE sets up access for a USER in accordance with the information provided by the REGULATOR.
5. The TRUST CENTRE sends the USER the SMART CARD, the assigned password, smart card software link and the address for the online portal by registered mail.
6. Upon confirmation of receipt of the password, the TRUST CENTRE sends the USER the PIN of the SMART CARD and the user ID by E-mail, so as to permit access.
7. The TRUST CENTRE informs the REGULATOR that access has been granted.

In the case of forgotten passwords or blocked access due to traceable reasons e.g. three failed attempts to enter the EMTOC password or SMART CARD PIN a new access will be established after verification of the reasons. The SMART CARD has to be send to the TRUST CENTRE.

In the case of a lost SMART CARD, the access will be deleted. A new access and SMART CARD will be reissued as described above with costs.



5.2 Data transmission process

After access has been granted, the USER can transmit files (uploading) and retrieve reports (downloading) via the online portal within a REPORTING PERIOD in accordance with his role. For this purpose, the following steps are necessary on each occasion:

1. Use of the SMART CARD in the card reader, with the entry of the appropriate PIN
2. Exchange of certificates via https (carried out automatically via a web browser)
3. Login via the secure connection, with entry of the user ID and secret password
4. Performance of possible operations:
    a. Mass upload of valid XML files (as compressed ZIP files)
    b. Entry of product INFORMATION via an online form
    c. Retrieval of reports on INFORMATION already submitted

Tools
Reporting parties who cannot independently generate valid XML files and whose products are too numerous for the manual input via the online form will be provided with a converter. The Excel2XML converter allows data to be entered in an Excel table, which corresponds to the harmonized templates of European Commission's Practical Guide on "Reporting on tobacco product ingredients". A valid XML file is generated in the required format via a macro, which can be transmitted by mass upload, as specified above. This tool is offered to USERS without any warranty as to the correctness or completeness of the XML file produced. The correctness and completeness are to be independently checked by the REPORTING PARTY by inspecting the transmission protocol received from EMTOC and by reviewing the reports generated automatically after transmission.

5.3 Assessment of the need for protection

To determine the need for protection of INFORMATION, the following classification is to be undertaken:

Possible risks arising from

- human errors: present, to be reduced by precise instructions, training and error-resistant software.
- technical errors: present, addressed by the IT security strategy, which includes software testing.
- deliberate abuse: present, since a financial incentive is given. The risks need to be countered by specific security measures (see Section 5.2).

Possible risks

- Confidentiality compromised: high
- Integrity compromised: high
- Availability compromised: not relevant

The need for protection of IT components is based on the possible damage that could arise as a result of malfunctions. The need for protection of CONFIDENTIAL INFORMATION is classified as normal (potential detrimental effects are limited and manageable) to high (potential detrimental effects could be considerable).
In the case of all measures for the protection of CONFIDENTIAL INFORMATION, the parties concerned should ensure that these are proportionate to the possible risks.

5.4 Security measures

The REPORTING PARTY is responsible for the security of INFORMATION prior to electronic transmission. After transmission, responsibility for the security of INFORMATION lies with the competent authority or designated administrator, who is to ensure security in accordance with the requisite IT security strategy. The level of protection specified in this Instruction is to be ensured by means of the attached "Requirements on the management of CONFIDENTIAL INFORMATION after transmission", or by comparable measures that ensures at least the same level of security. The security measures and strategy are confidential and will not be published.
For data transmission, storage and processing, aspects of data security as listed in the following table are to be taken into consideration. Potential threats to security can exist in many forms and those listed in the table are only some examples of what can occur. All USERS should be constantly alert to any potential threats to the security of the data or the security of the system and should put in place appropriate and adequate measures to address these threats.

No.	Potential threat	Required counter measure
1	Access to data storage facilities by unauthorised persons	Data storage area (servers, backup systems): the area is to be kept locked at all times and is only to be accessed with special task-related authorisation.
2.1	Accessing of data by unauthorised persons	INFORMATION can only be accessed by persons who have received authorisation in accordance with Section 6 of this Instruction. This also applies to REGULATORS' staff.
2.2		Accessing of data in the database is logged on each occasion.
2.3		The database is protected by a firewall.
2.4		Access to the database times out after a defined period of inactivity.
3	Interception of transmitted data, manipulation of data during transmission by third parties.	Use of https as encrypted data transmission protocol.
4	Delivery of data by unauthorised persons	Before the upload, authentication of the REPORTING PARTY via user ID and password is required. A report is only accepted if the MANUFACTURER data in the XML files matches the logged-in MANUFACTURER.
5.1	Publication of CONFIDENTIAL INFORMATION	INFORMATION that is to be published is supplied and stored in a separate file. Mixture of this INFORMATION with CONFIDENTIAL INFORMATION is therefore not possible. Only the INFORMATION intended for the general public is accessed, to generate the list for publication.
5.2		Immediately after submission, the REPORTING PARTY has the option of inspecting all his own lists in the form in which they are to be published.
6	Loss of CONFIDENTIAL INFORMATION after transmission	The requirements of the attached "Requirements on the management of CONFIDENTIAL INFORMATION after transmission" or equivalent security measures are to be complied with.
7.1	Damage caused by malware	The uploaded documents are checked. Only ZIP archives containing files in PDF or XML format are accepted.
7.2		The validity of the uploaded files is checked. Invalid files are rejected.
7.3		Known types of malicious attack are detected and repelled by the software (SQL injection, cross-site scripting, etc.).

6 Responsibilities

In this process, different tasks (roles) with different access rights are to be assigned. The roles are distinct, i.e. a USER cannot take on more than one role. The roles of REGULATOR, ADMINISTRATOR and TRUST CENTRE are to be assigned exclusively to the REGULATOR or to an authority appointed by the REGULATOR or prescribed by law. A table containing the established roles of the EMTOC system can be found in Annex II of this Instruction.

6.1 Responsibilities of the REGULATOR

6.1.1 Publication of information for the REPORTING PARTY

The appropriate contact address, the Terms of Use, the application forms for use of the EMTOC system and this Instruction are to be published, together with concomitant documents and the User Agreement, on the website of the REGULATOR or a centrally appointed institution. The responsible institutions acting as REGULATOR, administrator and TRUST CENTRE are indicated to the reporting parties.

6.1.2 Data management

- The REGULATOR ensures that the confidentiality of CONFIDENTIAL INFORMATION is maintained at all times during processing through its own IT strategy with the highest possible security standard.
- The REGULATOR processes and reviews the data in accordance with its legal mandate.
- The REGULATOR releases the INFORMATION submitted by law, for access by the EC.
- The REGULATOR informs the USERS concerned about incidents affecting the security of their own INFORMATION or general security aspects.
- The Regulator modulates or translates existing catalogue entries that have to be used by the USERS of his own Member State.
- The REGULATOR informs all USERS about a change of the procedure, security relevant system changes or format changes by e-mail or phone. The notification of changes of catalogue entries will be done automatically by the system.
- The REGULATOR is the only EMTOC instance that supports the USERS concerning EMTOC specific questions.

6.1.3 Publication of INFORMATION intended for the general public

INFORMATION is to be published on the REGULATOR'S website by the REGULATOR. The INFORMATION for the general public is made available as a PDF file or as an interactive list with a search function.

6.2 Responsibilities of the SYSTEM ADMINISTRATOR

The SYSTEM ADMINISTRATOR has the following responsibilities:

- Operation of the online portal, the server and database software

6.2.1 Operation of the data server

The SYSTEM ADMINISTRATOR operates the servers required by the system and is responsible for continuous monitoring and development of security standards. With regard to the storage of reporting parties' confidential documents, the SYSTEM ADMINISTRATOR manages the assigned areas (directories) and the assignment of access rights, so that protected areas are established for the reporting parties and the REGULATOR. In particular, the administrator performs the following tasks:

- Establishment of an access logging system (full audit trail), which records all authorised transactions (open/write in/copy/delete file) and all unauthorised attempts to access INFORMATION stored on the system. The SYSTEM ADMINISTRATOR makes this data available to the TRUST CENTRE for further evaluation.
- Evaluation of access log data in the event of irregularities.
- The SYSTEM ADMINISTRATOR blocks access for all USERS as quickly as possible, in cases where the database is suspected to have been compromised by unknown parties, until any threat to CONFIDENTIAL INFORMATION has been averted. The REGULATORS and the TRUST CENTRE are to be informed of such incidents.

6.2.2 Data management

- The SYSTEM ADMINISTRATOR ensures that the confidentiality of CONFIDENTIAL INFORMATION is maintained through its own IT strategy with the highest possible security standard.
- The SYSTEM ADMINISTRATOR ensures the integration of the submitted INFORMATION in a database.
- In this process of data handling and storage, the INFORMATION intended for publication is kept separate from the CONFIDENTIAL INFORMATION.
- With observation of the highest level of confidentiality, INFORMATION submitted to REGULATOR will be made available to the EC in accordance with its defined role.
- The SYSTEM ADMINISTRATOR ensures the data availability and integrity through sufficient backup systems. The data will be saved as backup once a day. The backup data will be store at least one year. The stored data is protected to prevent misuse in the event of theft of the used hardware. Backup hardware systems will be physically destroyed after the end of lifetime to avoid misuse of these data.

6.3 Responsibilities of the DATABASE ADMINISTRATOR

The DATABASE ADMINISTRATOR manages the reference catalogues of the database with the following responsibilities:

- Creation and maintenance of catalogues (Edition, Addition and Deletion of entries)
- Management of the list of confidential ingredients
- Changes and dissemination of XML schemas.

6.4 Responsibilities of the TRUST CENTRE

The central TRUST CENTRE manages USER access rights. This task also includes the cancellation of access rights and monitoring.

- The TRUST CENTRE grants USERS access to the system at the request of the REGULATOR.
- The TRUST CENTRE issues and manages the SMART CARDS.
- USER access rights are allocated exclusively to specified (named) individuals who access the system directly. However, USERS are to be specified by the responsible management of the relevant institution (REGULATOR or REPORTING PARTY).
- The TRUST CENTRE informs the administrator of any suspected abuse of a user ID.
- The TRUST CENTRE checks key points of the access log data received from the administrator.

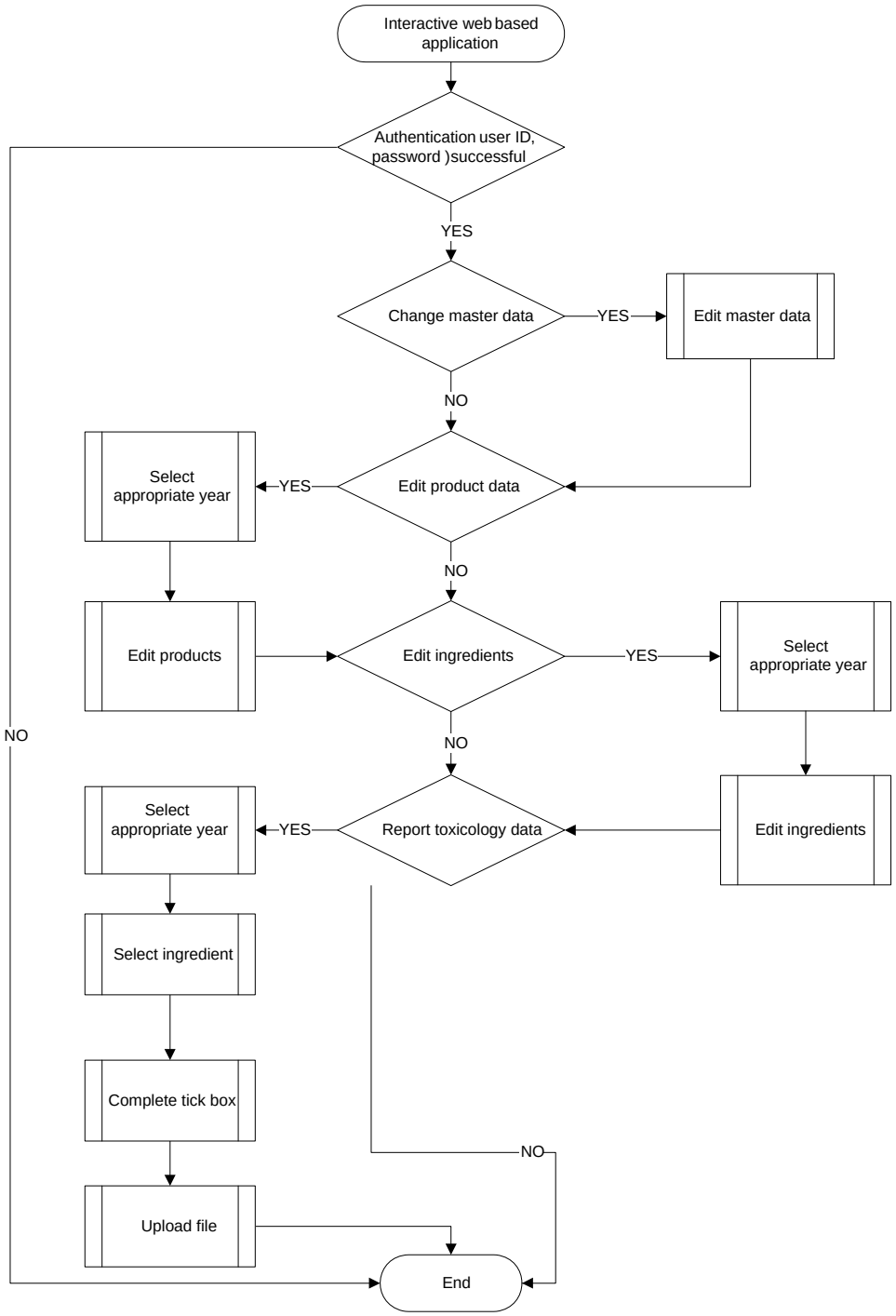
6.5 Responsibilities of reporting parties

- Specifying person responsible.
- Complying with the present Instruction and the concomitant documents.
- Uploading the required documents via the online portal within the REPORTING PERIOD.
- Checking the correctness of the INFORMATION transmitted in the automatically generated reports.
- Informing the REGULATOR about changes of address or a change of USER.
- Informing the REGULATOR and/or the TRUST CENTRE immediately in cases where abuse of the system or compromise of the user ID is suspected.
- Transfers the (yearly) fee for the use of EMTOC to the Trust Centre. Note that some member states have made deviant financial arrangements. In this case contact the REGULATOR of the member state.

7 Description of process

7.1 Procedure for exchange of CONFIDENTIAL INFORMATION

This section describes the procedure for the exchange of CONFIDENTIAL INFORMATION. This is only a schematically overview about the EMTOC procedure. The detailed description of the individual steps is described in the user manuals.



The required technical equipment is:

- PC with MS Windows
- Gemalto Card Reader (administrator rights required)
- Installed Driver for the Card Reader (administrator rights required)
- Installed encryption software TrueCrypt for data downloads by other USERS than REPORTING PARTIES
- Access to the world wide web (WWW)
- Internet browser MS Internet Explorer or Firefox (administrator rights required)

Furthermore it is necessary to have received after application:

- SMART CARD with PIN
- user name and password.

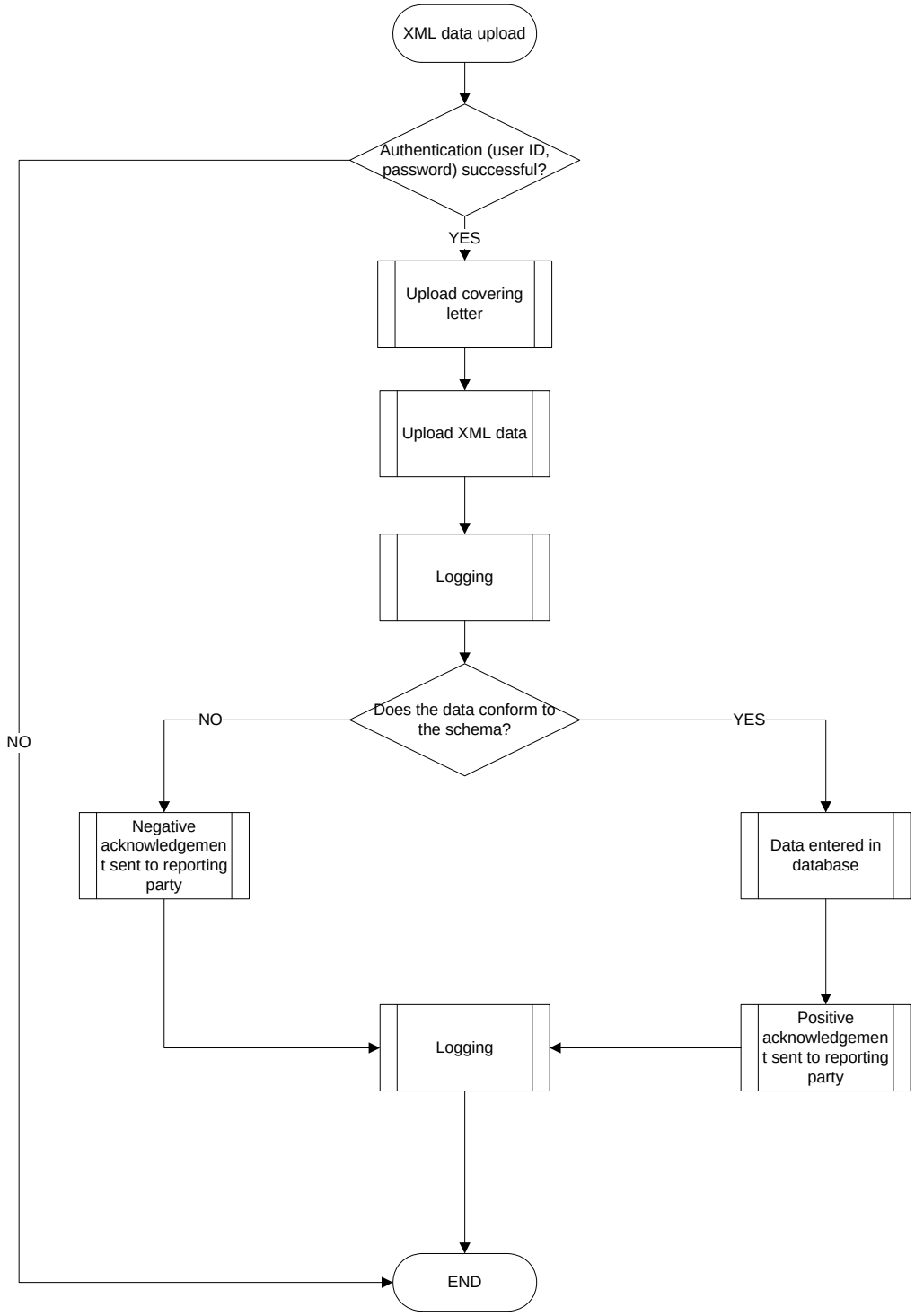
7.1.1 Upload of CONFIDENTIAL INFORMATION via online form

This is only possible for USERS registered as a REPORTING PARTY.

It is strongly recommended to upload the required information one week before the submission period ends.

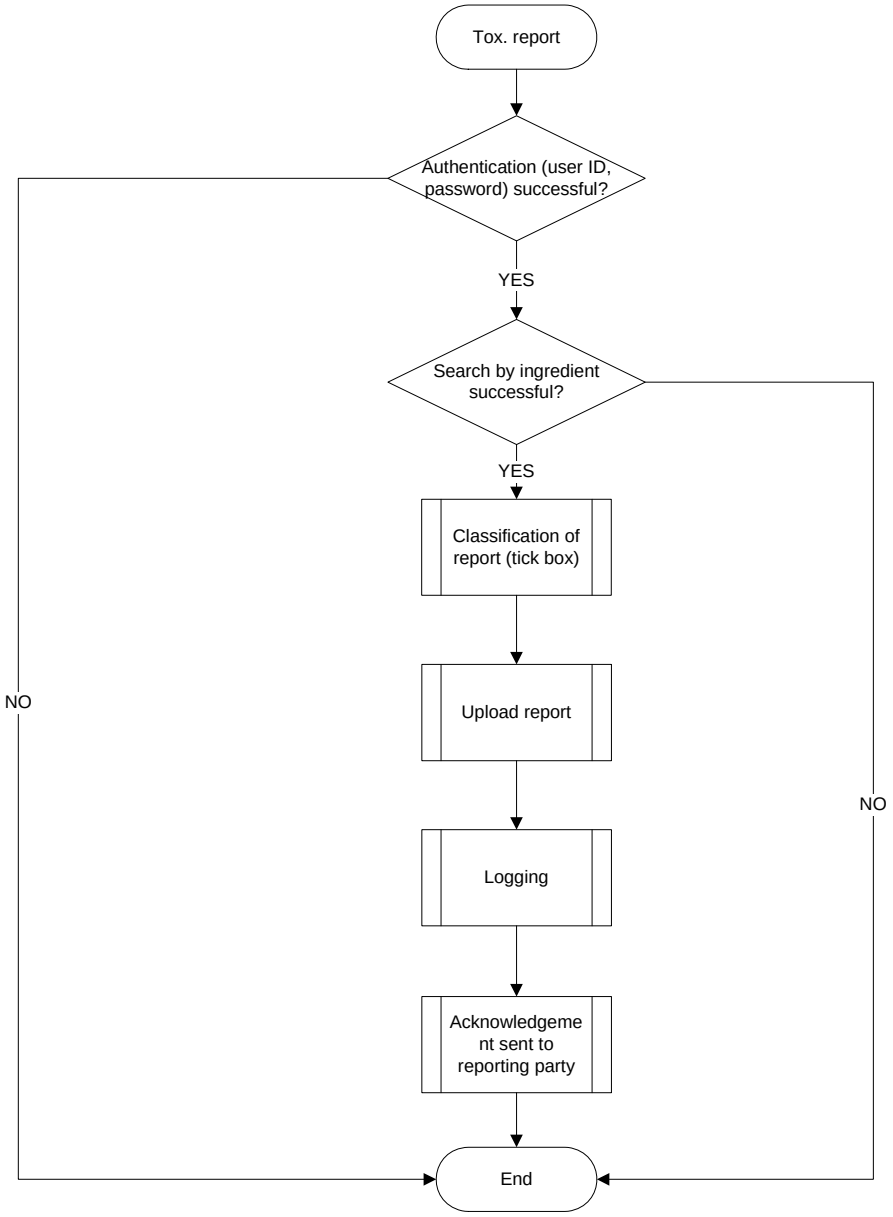
7.1.2 Bulk upload of CONFIDENTIAL INFORMATION

This is only possible for USERS registered as a REPORTING PARTY.



7.1.3 Upload of toxicology reports

This is only possible for USERS registered as a REPORTING PARTY.



7.1.4 Download of CONFIDENTIAL INFORMATION

This is only possible for registered authorised USERS: firstly, the REPORTING PARTY can only access its own INFORMATION; secondly, the REGULATOR of the Member State for which data is submitted. In addition, the EC can access CONFIDENTIAL INFORMATION in accordance with its defined role.

Procedure:

Downloading of INFORMATION from the system, by the REPORTING PARTY, corresponds to the creation of reports. Reports are generated as PDF files and can be stored locally. In order to ensure the security of downloaded INFORMATION, the requirements of the attached "Requirements on the management of CONFIDENTIAL INFORMATION after transmission" or equivalent security measures are to be complied with.

Downloading of data by the REGULATOR can also take the form of generation of reports as PDF files. Data can also be downloaded as XLS or CSV files for purposes of evaluation and review.

7.1.5 Editing of confidential documents

Editing of submitted INFORMATION is possible until the reporting deadline. Editing of any confidential data submitted from the Reporting Parties to the EMTOC system is restricted to Reporting Parties only. The management of reference catalogues is excluded from this restriction, since this has to be done by the database administrator.

Procedure:
As each new upload overwrites the preceding version, the INFORMATION submitted must always be complete. There is no limit to the number of uploads that may be carried out within the REPORTING PERIOD. Only the INFORMATION contained in the final upload is stored in the system.

Therefore, in order to edit individual items of INFORMATION (e.g. a product or an ingredient), changes can be made manually via the online form or a new submission with complete INFORMATION will have to be made.

7.1.6 Maintenance of the reference list of ingredients

The reference list of ingredients is maintained by the DATABASE ADMINISTRATOR who in principle will update the list once a year.
An EMTOC registration number (entry on the ingredient list) of competitively sensitive ingredient can be applied at the DATABASE ADMINISTRATOR. The DATABASE ADMINISTRATOR informs the applicant which EMTOC number has been assigned to the applied ingredient. All REGULATORS, but not REPORTING PARTIES, will be informed about the identity of the competitively sensitive ingredients in the EMTOC system. The competitively sensitive ingredients will appear in the reference list of ingredients as a number only.

7.2 Management of access information

- USERS receive their password, user ID and SMART CARD with PIN after submission of an application. System access information will be communicated separately by registered letters or personally, from the TRUST CENTRE.
- If any doubts arise concerning the authenticity of the letters, the REGULATOR has to be informed immediately.
- In the event of access information being lost, stolen or otherwise possibly falling into the hands of unauthorized third parties, the REGULATOR and the TRUST CENTRE are to be notified immediately.
- The TRUST CENTRE will block the access right of certain accounts if any kind of suspicion about unauthorized use of this account arises. The TRUST CENTRE will inform the responsible REGULATOR about the taken actions. The REGULATOR decides in cooperation with the TRUST CENTRE after contacting the concerned USER, if the account should be terminated or reopened.

7.3 Management of access via the online portal

- The Agreement concerning use of the online portal for reporting on tobacco product ingredients for the online portal is to be accepted in writing from all USERS (Annex). Access will only be granted when the User Agreement has been signed.
- The computer used for access is to be secured according to customary standards. If the computer has Internet access, it is to be protected at least by a firewall and an antivirus program.
- Documents are to be transmitted exclusively via an encrypted SSL connection, whereas unencrypted connections are to be cancelled immediately.

7.4 Compromise incidents

- If a server, computer, online access or file is found to have been compromised, the REGULATOR and/or the TRUST CENTRE should be informed immediately.
- The TRUST CENTRE will block a compromised access as quickly as possible.
- A compromised system is forensic evidence, and it must be possible for it to be made available to investigators unaltered. If a system has been compromised, it can no longer be used until the matter has been investigated.
- A compromised system can no longer be regarded as secure and reinstallation of the affected system is required in order to make it fully operational and usable.

7.5 Information from the REGULATOR

- USERS must provide the REGULATOR with an e-mail address, telephone and fax number that can be used to contact the USER or his/her deputy.
- USERS will receive confidential information either in encrypted form or by registered mail.
- Letters containing confidential information will always bear an official signature and be sent by registered mail.
- Urgent information, e.g. concerning security incidents, will be passed on immediately by telephone, e-mail or fax.
- Formulations or other CONFIDENTIAL INFORMATION will never be sent back to a REPORTING PARTY on another way as predetermined in the report modules of the EMTOC system (and not via e-mail, post mail or others).

7.6 Security incidents without compromisation

- Unless otherwise indicated, the REGULATOR is to be informed by the USER immediately of any deviations from this Instruction.
- Unless otherwise indicated, the REGULATOR is to be informed by the USER of any breaches of security.
- In the case of incidents affecting the security of CONFIDENTIAL INFORMATION, all events must be noted by the USER, with times being indicated as precisely as possible. These records are to be sent to the REGULATOR.
- If a security breach is suspected, USERS should behave as if the security breach had occurred.
- The REGULATOR informs the USERS concerned about security incidents in order to avert any threat to the security of CONFIDENTIAL INFORMATION.
- The REGULATOR immediately notifies the TRUST CENTRE of any information received or obtained concerning a threat to the security of the system. See also 7.2.

8 Concomitant documents

– This Instruction is without prejudice to REGULATORS' existing legal or procedural provisions, such as IT security requirements or employee confidentiality duties, which remain fully in force.

9 Annexes

- Annex I Requirements on the management of CONFIDENTIAL INFORMATION after transmission.

- Annex II Table about the roles of USERS in the EMTOC system and rights resulting from the responsibilities specified in section 6.

- Annex III User Agreement for the online portal. Online access authorisation requires acceptance of the terms and conditions of use.

Annex I: Requirements on the management of CONFIDENTIAL INFORMATION after transmission

1. Purpose

This document supplements the Instruction for electronic reporting on tobacco product ingredients via the Electronic Model Tobacco Control (EMTOC) system.

By following these requirements, it will be possible to comply with the requirements defined in the Instruction for the management of CONFIDENTIAL INFORMATION in connection with mandatory reporting on tobacco product ingredients. The determined technical instruments may be replaced by techniques that are offering the same level of protection.

2. Scope

The security and management of the EMTOC system are comprehensively regulated by the Instruction and concomitant documents. These requirements are therefore concerned with external access to the EMTOC system for the purpose of retrieving CONFIDENTIAL INFORMATION. They are applicable to all USERS of the EMTOC system and are to be regarded as supplementing the IT security strategies of USERS or their organisations. They cover all operations that can be carried out on the data by USERS of the EMTOC system after transmission. This includes downloading, storage, managing, printing, copying, forwarding, processing, evaluation and destruction of the data outside of the EMTOC system.

3. Requirements for compliance with data security as specified in the Instruction

3.1 Requirements for the computer system used to process CONFIDENTIAL INFORMATION

- On the computer used to access the EMTOC system, a powerful, up-to-date antivirus program must be installed. The hardware and software installation must be in accordance with the REGULATOR'S IT security strategy.

- A computer may only be used for processing EMTOC INFORMATION if access to data from this system can be securely restricted to duly authorised persons. In the case of a PC, this would be possible through the assignment of a BIOS password and system password or the use of a fingerprint reader or similar security measures.

- The data downloaded may only be stored on a local storage device (not on a server or online, for example). If a portable device is used, it must always be kept locked up when not in use.

- CONFIDENTIAL INFORMATION has to be stored solely in an encrypted form. It is not sufficient to password-protect Office documents or ZIP archives. The program recommended for standard use is TrueCrypt (www.truecrypt.org), which provides a securely encrypted drive for storage and processing of downloaded INFORMATION. It has to be ensured that files are saved directly to the encrypted drive and not temporarily stored elsewhere. When data is downloaded using a browser, the cache should subsequently be emptied as a precaution (e.g. using "Clear private data"). When documents

are deleted, it should be ensured that they are deleted permanently (not moved to the computer's recycle bin without emptying it). When Office software is used, the autosave function is to be disabled, or the encrypted drive should be set as the storage location.

3.2 Management of CONFIDENTIAL INFORMATION

- To access CONFIDENTIAL INFORMATION, it is necessary to download the data via a secured connection from the protected EMTOC system, using a user ID. Authorisation is granted to named individuals and must not be shared with others.

- CONFIDENTIAL INFORMATION should only be accessed to the minimum extent required.

- When using the EMTOC system, it is unnecessary to access confidential data in order to produce lists intended for publication or to forward INFORMATION to the European Commission. Confidential data should only be accessed to check completeness, correctness and timely delivery and, if appropriate, for statistical or toxicological evaluations.

- It is to be ensured that all CONFIDENTIAL INFORMATION downloaded to a computer after being processed, are irretrievably deleted.

3.3 Forwarding of CONFIDENTIAL INFORMATION

- In general, it is unnecessary for confidential data to be forwarded in any way. Should forwarding be necessary in principle on the basis of the REGULATOR'S internal requirements, the path is to be precisely defined and communicated to the reporting parties (together with the Instruction for use of the EMTOC system).

- CONFIDENTIAL INFORMATION transmitted in connection with electronic reporting on tobacco product ingredients via the EMTOC system may only be used as specified in the Instruction and should not under any circumstance be passed on to persons other than those authorised in accordance with the Instruction.

- Complete lists of individual reporting parties or those containing CONFIDENTIAL INFORMATION must not be printed out. For purposes of internal discussions involving authorised USERS and their relevant staff, individual pages may be printed out for immediate use but this should be subsequently destroyed using a cross-cut shredder. Printouts should be kept in a secure environment and destroyed either immediately after review or, at the latest, by the end of the working day of the printout. Printouts should not be removed from the secure environment in which they were printed.

- The sharing of INFORMATION as required by professional duties is allowed in cases where the data is aggregated and anonymised (without product relation).

- In general, the person registered as a USER for a REGULATOR is also responsible for the review and evaluation of CONFIDENTIAL INFORMATION. Should the need arise for involvement of additional authorised employees of the REGULATOR in the processing of CONFIDENTIAL INFORMATION, it is to be specified in writing which individuals have obtained access to the data, the time must be logged and the purpose is to be made clear.

Annex II: Table about the roles of USERS in the EMTOC system and rights resulting from the responsibilities specified in section 6

Role of a USER	**Responsibility**	**Rights**
REPORTING PARTY	Submission of required INFORMATION in a predefined format.	- Full access to the unlocked FOLDER (read, write, delete). - Uploading files to the unlocked FOLDER. - Downloading of reports on INFORMATION from the unlocked FOLDER.
REGULATOR	Review of INFORMATION submitted and creation of reports.	- Full read rights over all INFORMATION submitted for the REGULATOR'S Member State. - Change of existing catalogue entries for the own Member State (translations)
DATABASE ADMINISTRATOR	Creation and maintenance of catalogue entries and XML schemas.	- Creation, deletion or change of catalogue entries for all USER, which are stored separately from CONFIDENTIAL INFORMATION. - No access to CONFIDENTIAL INFORMATION within the system
SYSTEM ADMINISTRATOR	Responsible for EMTOC system hosting, maintaining and backups.	- Right to configure the hard- and software connected to the EMTOC system. - No access to the data within the EMTOC system.
TRUST CENTRE	USER management	- Assignment of personal user ID and of SMART CARDS with certificates. - Creation and deletion of USERS. - No access to INFORMATION submitted.
EC	Data evaluation	- The EC, like the REGULATOR, has full read rights over all INFORMATION. However, unlike the REGULATOR, the EC has access rights over the INFORMATION submitted for all Member States. If necessary, the EC is responsible for supranational evaluation.
Public	-	- No access to the database. - Viewing of published list of ingredients on national websites, excluding CONFIDENTIAL INFORMATION.

Annex III: Rules to be respected when the EMTOC system is used

The USER of EMTOC registered by the Trust Centre for EMTOC online access accepts the following terms and conditions of use:

1. Reporting on tobacco product ingredients necessitates the transmission of CONFIDENTIAL INFORMATION, which is only accessible to a small group of people. Hence, such data is to be treated always as confidential and must not be forwarded or made accessible to unauthorised persons under any circumstances.
2. The USER undertakes to use any confidential information received solely for the intended purpose and to comply with the data protection requirements. This obligation remains in effect after completion of the assigned tasks or termination of the employment contract.
3. The USER takes note of the Instruction for electronic reporting on tobacco product ingredients via the Electronic Model Tobacco Control (EMTOC) and all attachments and considers at his work the high degree of security needs of the confidential data.
4. The USER is to ensure a continuous update of the records of his/her personal contact details (business address, e-mail address, telephone and fax number) at the REGULATOR. The USER undertakes to inform the REGULATOR and the TRUST CENTRE immediately of the termination of his/her employment contract or of changes in his/her responsibilities.
5. Access data are to be kept secret and confidential to the USER. Passing on the user ID, password or the SMART CARD pin is prohibited. Only REPORTING PARTIES are allowed in own responsibility to share one USER access and SMART CARD between authorised persons (responsible person and his deputy). The USER is to ensure that it is impossible for unauthorised persons to access the system. Whenever the password becomes known to unauthorised persons, immediate blocking of access and a change of access data are to be requested.
6. The SMART CARD has only to be used with external card readers with independent pin pad and display. The SMART CARD has to be stored locked or kept at the body.
7. To protect the password and content, the online portal is not to be accessed with the user ID on public computers (e.g. Internet cafes, public libraries). The password saving option available in certain browsers must always be disabled.
8. Accessing the online portal with the user ID via an unsecured wireless network (WLAN) is prohibited.
9. Preset or initial passwords issued by the Trust Centre are to be changed at first login to individual secure passwords.
10. The USER accepts that the data intended for the submission to a specific REGULATOR will be stored at a centralized computer system in an EU member state.

Important Notes

- In case of inconsistencies or conflicts between the language in the EMTOC Instruction and the Terms of Use, the latter shall prevail.
- The signature, expressing full agreement with Annex III of the EMTOC Instruction, is to be given by all USERS (including REGULATORS an EC) on the EMTOC User agreement.