

Official Journal of the European Union

L 226



English edition

Legislation

Volume 64

25 June 2021

Contents

II *Non-legislative acts*

DECISIONS

- ★ **Decision (EU) 2021/1032 of the European Parliament of 27 April 2021 extending, by an additional period, the term of office of the Committee of Inquiry to investigate alleged contraventions and maladministration in the application of Union law in relation to the protection of animals during transport within and outside the Union** 1
- ★ **Decision No 1/2020 of the Joint Committee established by the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 5 November 2020 on the adoption of Common Operational Procedures (COP) [2021/1033]** 2
- ★ **Decision No 2/2020 of the Joint Committee established by the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 5 November 2020 on amending Annexes I and II to the Agreement and the adoption of Linking Technical Standards (LTS) (2021/1034)** 16
- ★ **Commission Implementing Decision (EU) 2021/1035 of 23 June 2021 amending Implementing Decisions 2013/648/EU and 2013/650/EU as regards the authorisation holder and its representative in the Union for the placing on the market of products containing, consisting of, or produced from certain genetically modified maize (notified under document C(2021) 4317) ⁽¹⁾** 31
- ★ **Commission Implementing Decision (EU) 2021/1036 of 22 June 2021 amending Implementing Decision (EU) 2018/1113 as regards the authorisation holder and its representative in the Union for the placing on the market of products produced from genetically modified sugar beet H7-1 (notified under document C(2021) 4325) ⁽¹⁾** 34
- ★ **Commission Implementing Decision (EU) 2021/1037 of 16 June 2021 on the request for registration of the European citizens' initiative entitled 'Ban Fossil Fuel Advertising and Sponsorships' pursuant to Regulation (EU) 2019/788 of the European Parliament and of the Council** 36

⁽¹⁾ Text with EEA relevance.

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

★ Commission Decision (EU) 2021/1038 of 23 June 2021 granting a transitional period to the Kingdom of the Netherlands pursuant to Decision 2008/477/EC as regards an update of relevant technical conditions applicable to the 2 500-2 690 MHz frequency band (notified under document C(2021) 4433)	38
--	----

III Other acts

EUROPEAN ECONOMIC AREA

★ Decision of the EEA Joint Committee No 130/2021 of 15 March 2021 amending Protocol 10 to the EEA Agreement, on simplification of inspections and formalities in respect of carriage of goods [2021/1039]	41
--	----

II

(Non-legislative acts)

DECISIONS

DECISION (EU) 2021/1032 OF THE EUROPEAN PARLIAMENT

of 27 April 2021

extending, by an additional period, the term of office of the Committee of Inquiry to investigate alleged contraventions and maladministration in the application of Union law in relation to the protection of animals during transport within and outside the Union

THE EUROPEAN PARLIAMENT,

- having regard to the proposal by the Conference of Presidents,
 - having regard to Article 226 of the Treaty on the Functioning of the European Union,
 - having regard to Decision 95/167/EC, Euratom, ECSC of the European Parliament, the Council and the Commission of 19 April 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry ⁽¹⁾,
 - having regard to its Decision (EU) 2020/1089 of 19 June 2020 on setting up a committee of inquiry to investigate alleged contraventions and maladministration in the application of Union law in relation to the protection of animals during transport within and outside the Union, and defining its responsibilities, numerical strength and term of office ⁽²⁾,
 - having regard to its Decision (EU) 2021/429 of 20 January 2021 extending the term of office of the Committee of Inquiry to investigate alleged contraventions and maladministration in the application of Union law in relation to the protection of animals during transport within and outside the Union ⁽³⁾,
 - having regard to Rule 208(11) of its Rules of Procedure,
- A. whereas the Committee of Inquiry requested a second extension of its term of office in order to be allowed to fully and correctly fulfil its mandate;
1. Decides to extend by an additional period of three months the term of office of the Committee of Inquiry.

*For the European Parliament**The President*

D. M. SASSOLI

⁽¹⁾ OJ L 113, 19.5.1995, p. 1.

⁽²⁾ OJ L 239 I, 24.7.2020, p. 1.

⁽³⁾ OJ L 86, 12.3.2021, p. 1.

**DECISION No 1/2020 OF THE JOINT COMMITTEE ESTABLISHED BY THE AGREEMENT
BETWEEN THE EUROPEAN UNION AND THE SWISS CONFEDERATION ON THE LINKING OF
THEIR GREENHOUSE GAS EMISSIONS TRADING SYSTEMS**

of 5 November 2020

on the adoption of Common Operational Procedures (COP) [2021/1033]

THE JOINT COMMITTEE,

Having regard to the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems ⁽¹⁾ ('the Agreement') and in particular Article 3(6) thereof,

Whereas:

- (1) Decision No 2/2019 of the Joint Committee of 5 December 2019 ⁽²⁾ amended Annexes I and II to the Agreement thus fulfilling the conditions for linking set out in the Agreement.
- (2) Following adoption of Decision No 2/2019 of the Joint Committee and pursuant to Article 21(3) of the Agreement, the Parties exchanged their instruments of ratification or approval, since they consider all conditions for linking as set out in the Agreement to have been fulfilled.
- (3) In accordance with Article 21(4) of the Agreement, the Agreement entered into force on 1 January 2020.
- (4) Pursuant to Article 3(6) of the Agreement, the Swiss registry administrator and the Union central administrator should determine common operational procedures (COP) related to technical or other matters necessary for the operation of the link between the European Union Transaction Log (EUTL) of the Union registry and the Swiss Supplementary Transaction Log (SSTL) of the Swiss registry and taking into account the priorities of domestic legislation. The COP should take effect when adopted by decision of the Joint Committee.
- (5) In accordance with Article 13(1) of the Agreement, the Joint Committee should agree on technical guidelines to ensure the proper implementation of the Agreement including on technical or other matters necessary for the operation of the linking and taking into account the priorities of domestic legislation. Technical guidelines may be developed by a working group set up pursuant to Article 12(5) of the Agreement. The working group should at least include the Swiss registry administrator and the Union central administrator and should assist the Joint Committee in its functions under Article 13 of the Agreement.
- (6) In view of the technical nature of the guidelines and the need to adapt them to ongoing developments, the technical guidelines developed by the Swiss registry administrator and the Union central administrator should be submitted to the Joint Committee for information or, where appropriate, approval,

HAS ADOPTED THIS DECISION:

Article 1

The Common Operational Procedures (COP), as annexed to this Decision, are hereby adopted.

⁽¹⁾ OJ L 322, 7.12.2017, p. 3.

⁽²⁾ Decision No 2/2019 of the Joint Committee established by the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 5 December 2019 amending Annexes I and II to the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems (OJ L 314, 29.9.2020, p. 68).

Article 2

Herewith, a working group shall be set up pursuant to Article 12(5) of the Agreement. It shall assist the Joint Committee in ensuring the proper implementation of the Agreement, including the development of technical guidelines for the implementation of the COP.

The working group shall at least include the Swiss registry administrator and the Union central administrator.

Article 3

This Decision shall enter into force on the date of its adoption.

Done at Brussels, 5 November 2020.

For the Joint Committee

Secretary for the European Union
Maja-Alexandra DITTEL

The Chair
Beatriz YORDI

Secretary for Switzerland
Caroline BAUMANN

ANNEX

Common operational procedures (COP) pursuant to Article 3(6) of the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems

PROCEDURES FOR PROVISIONAL SOLUTION

1. **Glossary**

Table 1-1

Acronyms and Definitions

Acronym/Term	Definition
Certificate Authority (CA)	Entity that issues digital certificates.
CH	Swiss Confederation
ETS	Emissions Trading System
EU	European Union
IMT	Incident Management Team
Information Asset	A piece of information that is valuable to a company or organization.
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
LTS	Linking Technical Standards
Registry	An accounting system for allowances issued under the ETS, which keeps track of the ownership of allowances held in electronic accounts.
RFC	Request For Change
SIL	Sensitive Information List
SR	Service Request
Wiki	Website that allows users to exchange information and knowledge by adding or adapting content directly via a web browser.

2. **Introduction**

The Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 23 November 2017 ('Agreement') provides for the mutual recognition of emission allowances that can be used for compliance under the Emissions Trading System of the European Union ('EU ETS') or the Emissions Trading System of Switzerland ('ETS of Switzerland'). To operationalise the link between the EU ETS and the ETS of Switzerland, a direct link between the European Union Transaction Log (EUTL) of the Union Registry and the Swiss Supplementary Transaction Log (SSTL) of the Swiss registry will be established, which will enable the registry-to-registry transfer of emission allowances issued under either ETS (Article 3(2) of the Agreement). To operationalise the link between the EU ETS and the ETS of Switzerland, a provisional solution shall be in place by May 2020 or as soon as possible thereafter. Parties shall cooperate to replace the provisional solution with a permanent registry link as soon as possible (Annex II to the Agreement).

Pursuant to Article 3(6) of the Agreement, the Swiss registry administrator and the Union central administrator shall determine common operational procedures (COP) related to technical or other matters necessary for the operation of the linking and taking into account the priorities of domestic legislation. The COP developed by the administrators shall take effect when adopted by decision of the Joint Committee.

The COP, as recorded in this document, is to be adopted by the Joint Committee by its Decision No 1/2020. In accordance with this Decision, the Joint Committee shall request the Swiss registry administrator and the Union central administrator to develop further technical guidelines to operationalise the link and to ensure that these are continuously adapted to technical progress and new requirements relating to the safety and security of the link and to its effective and efficient operation.

2.1. *Scope*

This document represents the common understanding between the Parties to the Agreement regarding the establishment of the procedural foundations of the link between the registries of the EU ETS and the ETS of Switzerland. While it outlines the overall procedural requirements in terms of operations, some further technical guidelines will be needed to operationalise the link.

For its proper functioning, the link will require technical specifications in order to further operationalise it. Pursuant to Article 3(7) of the Agreement, those matters are detailed in the Linking Technical Standards (LTS) document to be adopted separately by decision of the Joint Committee.

The objective of the COP is to make sure that IT services related to the operation of the link between the registries of the EU ETS and the ETS of Switzerland are delivered effectively and efficiently, especially for the fulfilling of service requests, resolving service failures, fixing problems, as well as carrying out routine operational tasks according to international standards for IT service management.

For the agreed provisional solution, only the following COP will be needed, which are part of this document:

- Incident Management;
- Problem Management;
- Request Fulfilment;
- Change Management;
- Release Management;
- Security Incident Management;
- Information Security Management.

With the deployment of the permanent registry link at a later date, the COP must be adapted and supplemented where necessary.

2.2. *Addressees*

The target audience of these COP are the EU and Swiss registry support teams.

3. **Approach and Standards**

The following principle applies to all COP:

- The EU and CH agree to define the COP on the basis of ITIL (Information Technology Infrastructure Library, version 3). Practices from this standard are reused and adapted to the specific needs related to the provisional solution;
- The communication and coordination necessary for the processing of the COP between the two Parties takes place via the Registry Service Desks of the CH and EU. Tasks are always assigned within one Party;
- If there is disagreement about the handling of a COP, this will be analysed and resolved between both Service Desks. If no agreement can be reached, the finding of a joint solution is escalated to the next level.

Escalation levels	EU	CH
1st level	EU Service Desk	CH Service Desk
2nd level	EU Operations Manager	CH Registry Application Manager
3rd level	Joint Committee (which might delegate this responsibility considering Article 12(5) of the Agreement)	
4th level	Joint Committee, if 3rd level is delegated	

;

- Each Party can determine the procedures for the operation of its own registry system, taking into account the requirements and interfaces related to these COP;
- An IT Service Management (ITSM) tool is used to support the COP, in particular Incident Management, Problem Management and Request Fulfilment, and communication between both Parties;
- In addition, the exchange of information via e-mail is allowed;
- Both Parties ensure that the information security requirements are met in accordance with the Handling Instructions.

4. Incident management

The objective of the Incident Management process is to return IT services to a normal service level as quickly as possible following an incident and with minimum disruption to the business.

Incident Management should also keep a record of incidents for reporting purposes and integrate with other processes to drive continuous improvement.

From a global perspective, Incident Management comprises the following activities:

- Incident detection and recording;
- Classification and initial support;
- Investigation and diagnosis;
- Resolution and recovery;
- Incident closure.

Throughout the lifecycle of an incident, the Incident Management process is responsible for the constant handling of the ownership, monitoring, tracking and communication.

4.1. Incident detection and recording

An incident can be detected by a support group, by automated monitoring tools or by technical staff performing routine surveillance.

Once detected, an incident must be recorded and assigned a unique identifier allowing for proper incident tracking and monitoring. The unique identifier of an incident is the identifier assigned in the common ticketing system by the Service Desk of the Party (either EU or CH) that raised the incident, and it has to be used in every communication related to this incident.

For all incidents, the contact point should be the Service Desk of the Party that logged the ticket.

4.2. Classification and initial support

The incident classification aims at understanding and identifying what system and/or service are affected by an incident, and to what degree. To be effective, the classification should route the incident to the correct resource on the first try, in order to speed up the incident resolution.

The classification phase should categorize and prioritize the incident according to its impact and urgency, for it to be treated according to the priority relevant time frame.

If the incident has a potential impact on the confidentiality or integrity of sensitive data, and/or an impact on the system availability, the incident shall be also declared as a security incident and then managed according to the process defined in the 'Security Incident Management' chapter of this document.

If possible, the Service Desk that logged the ticket performs an initial diagnosis. For this, the Service Desk will see if the incident is a known error. If so, then the resolution path or workaround is already known and documented.

If the Service Desk is successful in solving the incident, then it will actually close the incident at this point, as the primary purpose of Incident Management has been fulfilled (namely the fast restoration of service for the end user). If not, then the Service Desk will escalate the incident to the appropriate resolver group for further investigation and diagnosis.

4.3. *Investigation and diagnosis*

Incident investigation and diagnosis is applied when an incident cannot be resolved by the Service Desk as part of the initial diagnosis, and is therefore escalated appropriately. Incident escalation is a full part of the investigation and diagnosis process.

A common practice in the investigation and diagnosis phase is the attempt to recreate the incident under controlled conditions. It is important when performing incident investigation and diagnosis that the proper order of events that led up to the incident be understood.

Escalation is the recognition that an incident cannot be resolved at the current support level, and must be passed to a higher level support group or to the other Party. Escalation can follow two paths: horizontal (functional) or vertical (hierarchical).

The Service Desk that recorded and triggered the incident is responsible for escalating the incident to the appropriate resource and for tracking the overall status and assignment of the incident.

The Party to which the incident has been assigned is responsible for ensuring the requested actions are performed in a timely fashion, and for providing feedback to the Service Desk of its own Party.

4.4. *Resolution and recovery*

Incident resolution and recovery is performed once the incident is fully understood. Finding a resolution to an incident means that a way of rectifying the issue has been identified. The act of applying the resolution is the recovery phase.

Once the appropriate resources resolve the service failure, the incident is routed back to the relevant Service Desk that logged the incident and that Service Desk confirms with the initiator of the incident that the error has been rectified and that the incident can be closed. Findings from the processing of the incident are to be recorded for future use.

Recovery can be performed by IT support staff or by providing the end user with a set of instructions to follow.

4.5. *Incident closure*

Closure is the final step in the Incident Management process and takes place shortly after incident resolution.

Within the checklist of activities that need to be performed during the closure phase, the following are highlighted:

- The verification of the initial categorization that was assigned to the incident;
- The proper capture of all information surrounding the incident;
- The proper documentation of the incident and update of the knowledge base;
- The adequate communication to every stakeholder directly or indirectly affected by the incident.

An incident is formally closed once the incident closure phase has been executed by the Service Desk and communicated to the other Party.

Once an incident is closed, it is not reopened. If an incident re-occurs within a short time period then, the original incident is not re-opened, a new incident must be logged instead.

If the incident is tracked by both the EU and CH Service Desks, the final closure is the responsibility of the Service Desk that logged the ticket.

5. **Problem Management**

This procedure should be followed whenever a problem is identified and therefore triggers the Problem Management process. Problem Management focuses on enhancing quality and reducing the volume of raised incidents. A problem can be the cause of one or more incidents. When an incident is reported, the objective of Incident Management is to restore the service as quickly as possible, possibly involving workarounds. When a problem is created, the objective is to investigate the root cause of the issue in order to identify a change that will ensure the problem and related incidents will not occur anymore.

5.1. *Problem identification and recording*

Depending on which Party initiated the ticket, either the EU or CH Service Desk will be the contact point for problem related matters.

The unique identifier of a problem is the identifier assigned by the IT Service Management (ITSM). It has to be used in every communication related to this problem.

A problem can be triggered by an incident or can be opened as a self-initiative act to fix issues discovered in the system at any point in time.

5.2. *Problem Prioritization*

Problems may be categorized according to their severity and priority in the same way as incidents in order to facilitate their tracking, taking the impact of the associated incidents and their frequency of occurrence into account.

5.3. *Problem investigation and diagnosis*

Each Party can raise a problem and the Service Desk of the initiating Party will be responsible for logging the problem, assigning it to the appropriate resource and tracking the overall status of the problem.

The resolver group to whom the problem was escalated is responsible for handling the problem in a timely fashion and communicating with the Service Desk.

Upon request, both Parties are responsible for ensuring the assigned actions are performed, and for providing feedback to the Service Desk of its own Party.

5.4. *Resolution*

The resolver group to whom the problem is assigned is responsible for resolving the problem and providing relevant information to the Service Desk of its own Party.

Findings from the processing of the problem are to be recorded for future use.

5.5. *Problem closure*

A problem is formally closed once the problem is fixed by implementing the change. The problem closure phase will be carried out by the Service Desk that logged the problem and informed the Service Desk of the other Party.

6. **Request Fulfilment**

The Request Fulfilment Process is the end-to-end management of a request for a new or existing service from the moment it is registered and approved through to closure. Service Requests are usually small, predefined, repeatable, frequent, pre-approved, and procedural requests.

The main steps that have to be followed are outlined below:

6.1. *Initiate Request*

The information related to a Service Request is submitted to the EU or CH Service Desk by email, phone, or through the IT Service Management (ITSM) tool or any other agreed channel of communication.

6.2. *Request Logging and Analysis*

For all Service Requests, the contact point should be the EU or CH Service Desk, depending on which Party raised the Service Request. This Service Desk will be responsible for logging and analysing the Service Request with the appropriate diligence.

6.3. *Request Approval*

The Service Desk Agent of the Party that raised the Service Request checks if any approvals are required from the other Party and if so proceeds to obtain them. If the Service Request is not approved, the Service Desk updates and closes the ticket.

6.4. *Request fulfilment*

This step caters for the effective and efficient handling of Service Requests. A distinction must be made between the following cases:

- The fulfilment of the Service Request only affects one Party. In this case, this Party issues the work orders and coordinates the execution.
- The fulfilment of the Service Request affects both the EU and CH. In this case, the Service Desks issue the work orders in their area of responsibility. The processing of the Service Request fulfilment is coordinated between both Service Desks. The overall responsibility lies with the Service Desk that received and initiated the Service Request.

When the Service Request has been fulfilled, it must be placed into Resolved State.

6.5. *Request Escalation*

The Service Desk can escalate the outstanding Service Request to the appropriate resource (third Party) if needed.

Escalations are done to the respective third Parties, i.e. the EU Service Desk will have to go through the CH Service Desk for escalation to a CH third Party, and vice versa.

The third Party to whom the Service Request was escalated is responsible for handling the Service Request in a timely fashion and communicating with the Service Desk who escalated the Service Request.

The Service Desk that logged the Service Request is responsible for tracking the overall status and assignment of a Service Request.

6.6. *Request Fulfilment Review*

The responsible Service Desk submits the Service Request Record to a final quality control before it is closed. The aim is to make sure that the Service Request is actually processed and that all information required to describe the request's life-cycle is supplied in sufficient detail. In addition to this, findings from the processing of the request are to be recorded for future use.

6.7. *Request Closure*

If the assigned Parties agree that the Service Request has been fulfilled and the requestor considers the case resolved, the next status to be set is 'Closed'.

A Service Request is formally closed once the Service Desk that logged the Service Request has executed the request closure phase and informed the Service Desk of the other Party.

7. **Change Management**

The objective is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. Changes in IT infrastructure may arise reactively in response to problems or externally imposed requirements, e.g. legislative changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives.

The Change Management process includes different steps that capture every detail about a Change Request for future tracking. These processes ensure that the change is validated and tested before it moves to deployment. The Release Management process is responsible for successful deployment.

7.1. *Request for Change*

A Request For Change (RFC) is submitted to the Change Management team for validation and approval. For all Change Requests, the contact point should be the EU or CH Service Desk, depending on which Party raised the request. This Service Desk will be responsible for logging and analysing the request with appropriate diligence.

Change Requests may originate from:

- An incident that causes a change;
- An existing problem that results in a change;
- An end user requesting for a new change;
- Change as a result of an ongoing maintenance;
- Legislative change.

7.2. *Change Evaluation and Planning*

This stage handles change assessment and planning activities. It includes prioritization and planning activities to minimize risk and impact.

If the implementation of the RFC affects both the EU and CH, the Party that logged the RFC verifies the change evaluation and planning with the other Party.

7.3. *Change approvals*

Any registered change request needs to be approved by the relevant escalation level.

7.4. *Change implementation*

Change implementation is handled in the Release Management process. The Release Management teams of both Parties follow their own processes that involve planning and testing. Change review happens once the implementation is completed. To ensure that everything has gone according to plan the existing Change Management process is constantly reviewed and updated wherever necessary.

8. **Release Management**

A release represents one or more changes to an IT service, collected in a release plan that will have to be authorized, prepared, built, tested, and deployed together. A release may represent a bug fix, a change to hardware or other components, changes to software, upgrades of application versions, changes to documentation and/or processes. The contents of each release are managed, tested and deployed as a single entity.

Release Management aims to plan, build, test and validate, and deliver capability to provide the designed services, which will accomplish the stakeholders' requirements and deliver the intended objectives. Acceptance criteria for all changes to the service will be defined and documented during design coordination and provided to Release Management teams.

The release will typically consist of a number of problem fixes and enhancements to a service. It contains the new or changed software required and any new or changed hardware needed to implement the approved changes.

8.1. *Plan the release*

The first step of the process assigns authorized changes to release packages and defines the scope and content of releases. Based on this information, the Release Planning sub-process develops a schedule for building, testing and deploying the release.

Planning should define:

- Scope and content of the release;
- Risk assessment and risk profile for the release;
- Customer/users affected by the release;
- Team responsible for the release;
- Delivery and deployment strategy;
- Resources for the release and its deployment.

Both Parties inform each other about their release planning and maintenance windows. If a release affects both the EU and CH, they coordinate the planning and define a common maintenance window.

8.2. *Build and Test Release Package*

The build and test step of the Release Management process establishes the approach of executing the release or release package and of maintaining the controlled environments prior to changing production, as well as testing all changes in all environments released.

If a release affects both the EU and CH, they coordinate the delivery plans and tests. This includes the following aspects:

- How and when release units and service components will be delivered;
- What the typical lead times are; what happens if there is a delay;
- How to track the progress of the delivery and obtain confirmation;
- Metrics for monitoring and determining the success of the release deployment effort;
- Common test cases for relevant functionalities and changes.

At the end of this sub-process, all required release components are ready to enter the live deployment phase.

8.3. *Prepare deployment*

The preparation sub-process ensures that communication plans are defined correctly and notifications are ready to be sent to all stakeholders and end users impacted, and that the release is integrated with the Change Management process to ensure that all changes are performed in a controlled manner and approved by the required forums.

If a release affects both the EU and CH, they shall coordinate the following activities:

- Change Request record for scheduling and preparing deployment to Production environment;
- Create implementation plan;
- Rollback approach, so that, in case of deployment failure, the previous state can be placed back;
- Notifications sent to all necessary Parties;
- Require approval for the implementation of the release from the relevant escalation level.

8.4. *Roll back the release*

In case deployment has failed or testing has identified that deployment was unsuccessful or has not met the agreed acceptance/quality criteria, the Release Management teams of both Parties will need to roll back to the previous state. All necessary stakeholders will need to be informed, including impacted/targeted end users. Pending approval, the process can restart at any of the previous stages.

8.5. *Review and close release*

When reviewing a deployment, the following activities should be included:

- Capture feedback on customer, user and service delivery satisfaction with the deployment (collect the feedback and consider for continuously improving the service);
- Review any quality criteria that were not met;
- Check that any actions, necessary fixes and changes are complete;
- Make sure there are no capability, resource, capacity or performance issues at the end of the deployment;
- Check that any problems, known errors and workarounds are documented and accepted by the customer, end users, operational support, and other Parties impacted;
- Monitor incidents and problems caused by deployment (provide early life support to operational teams in case the release has caused an increase in volumes of work);
- Update support documentation (i.e. technical information documents);
- Formally hand over the release deployment to service operations;
- Document lessons learnt;
- Collect the release summary document from implementation teams;
- Formally close the release after verifying the Change Request record.

9. **Security Incident Management**

Security Incident Management is a process for handling security incidents in order to enable incident communication to potentially impacted stakeholders; incident evaluation and prioritisation; and incident response to settle any actual, suspected or potential breach of confidentiality, availability or integrity of sensitive information assets.

9.1. *Information Security Incident Categorization*

All incidents impacting the link between the Union Registry and the Swiss registry shall be analysed to determine a possible breach in the confidentiality, the integrity or the availability of any sensitive information recorded in the Sensitive Information List (SIL).

If so, the incident shall be characterized as an information security incident, immediately registered in the IT Service Management (ITSM) tool and managed as such.

9.2. *Information Security Incident Handling*

Security Incidents are placed under the responsibility of the 3rd escalation level and resolution of the incidents will be dealt with by a dedicated Incident Management Team (IMT).

The IMT is responsible for:

- Carrying out a first analysis, categorizing and rating the severity of the incident;
- Coordinating actions between all the stakeholders including the full documentation of the incident analysis, the decisions taken to tackle the incident and any possible identified weaknesses;
- Depending on the severity of the security incident, escalating the incident in a timely manner to the appropriate level for information and/or a decision.

In the Information Security Management process, all information regarding incidents is classified at the highest level of sensitivity of the information, but in any case not lower than ETS SENSITIVE.

For an on-going investigation and/or a weakness that could be exploited, and until its remediation, the information is classified as ETS CRITICAL.

9.3. *Security Incident Identification*

Based on the security event type, the information security officer determines appropriate organizations to be involved and to be part of the IMT.

9.4. *Security Incident Analysis*

The IMT liaises with all involved organizations and the relevant members of their teams, as appropriate, to review the incident. During the analysis, the extent of an asset's confidentiality, integrity or availability loss is identified and consequences for all affected organizations are assessed. Next, initial and follow-up actions to resolve the incident and manage its impact, including the resource impact of these actions, are defined.

9.5. *Security Incident Severity assessment, Escalation and Reporting*

The IMT shall assess the severity of any new security incident after its characterization as a security incident and shall start immediate required action according to the severity of the incident.

9.6. *Security Response Reporting*

The IMT includes incident containment and recovery results in the information security incident response report. The report is provided to the 3rd escalation level using secure email or other mutually accepted means of secure communication.

The responsible Party reviews the containment and recovery results and:

- Reconnects the registry in case of prior disconnection;
- Provides incident communications to the registry teams;
- Closes the incident.

The IMT should include – in a secure manner - relevant details in the information security incident report in order to ensure consistent recording and communication and to enable prompt and appropriate action to contain the incident. Following its completion, the IMT provides the information security incident final report in due course.

9.7. *Monitoring, Capacity Building and Continuous Improvement*

The IMT will provide reports for all security incidents to the 3rd escalation level. The reports will be used by this escalation level to determine the following:

- Weak points in security controls and/or operation that need to be strengthened;
- A possible need to enhance this procedure to improve the effectiveness of the response to incidents;
- Training and capacity building opportunities to further strengthen the information security resilience of registry systems, reduce the risk of future incidents and minimize their impact.

10. **Information Security Management**

Information Security Management aims to ensure the confidentiality, integrity and availability of an organization's classified information, data and IT services. In addition to the technical components including their design and testing (see LTS), the following common operational procedures are necessary to fulfil the security requirements for the provisional solution.

10.1. *Sensitive information identification*

The sensitivity of a piece of information is assessed by determining the level of impact on the business (e.g. financial losses, image degradation, law infringement...) a security breach related to this information could have.

The sensitive information assets shall be identified on the basis of their impact on linking.

The level of sensitivity of this information shall be assessed according to the sensitivity scale applicable for this linking and detailed in the 'Information Security Incident Handling' section of this document.

10.2. *Sensitivity levels of Information Assets*

Upon its identification, the information asset is classified by applying the following rules:

- The identification of at least a single HIGH confidentiality, integrity or availability level classifies the asset as ETS CRITICAL;
- The identification of at least a single MEDIUM confidentiality, integrity or availability level classifies the asset as ETS SENSITIVE;
- The identification of only LOW confidentiality, integrity or availability levels classifies the asset as ETS LIMITED.

10.3. *Assignment of Information Assets Owner*

All information assets should have an assigned owner. Information assets of the ETS, belonging to or in conjunction with the link between the EUTL and the SSTL should be included in a joint asset inventory list, maintained by both Parties. Information assets of the ETS outside the link between the EUTL and the SSTL should be included in an asset inventory list, maintained by the respective Party.

Ownership of each information asset belonging to or in conjunction with the link between the EUTL and the SSTL is to be agreed to by the Parties. The owner of an information asset is responsible for assessing its sensitivity.

The owner should have a level of seniority that is appropriate to the value of the assigned asset(s). The owner's responsibility for the asset(s) and his or her obligation to maintain the required level of confidentiality, integrity and availability should be agreed and formalized.

10.4. *Registration of sensitive information*

All sensitive information shall be registered in the Sensitive Information List (SIL).

Where relevant, the aggregation of sensitive information that could lead to a higher impact than the impact of one single piece of information shall be taken into account and registered in the SIL (e.g. a set of information stored in the system database).

The SIL is not static. Threats, vulnerabilities, likelihood or consequences of security incidents related to the assets may change without any indication and new assets might be introduced into the operation of registry systems.

Therefore, the SIL shall be reviewed regularly and any new information identified as sensitive shall be immediately registered into the SIL.

The SIL shall contain at least the following information for each entry:

- Description of the information
- Information owner
- Sensitivity level
- Indication if the information includes personal data
- Additional information if required

10.5. *Handling of sensitive information*

When processed outside the link between the Union Registry and Swiss Registry, sensitive information shall be handled in accordance with the Handling Instructions.

Sensitive information processed by link between the Union Registry and Swiss Registry shall be handled in accordance with the Security requirements by the Parties.

10.6. *Access Management*

The objective of Access Management is to grant authorized users the right to use a service, while preventing access to non-authorized users. Access Management is sometimes also referred to as 'Rights Management' or 'Identity Management'.

For the provisional solution and its operation, both Parties need access to the following components:

- Wiki: A collaboration environment for the exchange of common information, such as release planning;
- IT Service Management (ITSM) Tool for incident and problem management (see chapter 3, 'Approach and Standards');
- Message exchange system: each Party shall provide a secure message exchange transfer system for the transmission of the messages containing the transaction data.

The Swiss registry administrator and the Union central administrator ensure that accesses are up-to-date and act as contact points for their Parties for access management activities. Access requests are handled according to the Request Fulfilment procedures.

10.7. *Certificate/Key Management*

Each Party is responsible for its own certificate/key management (generation, registration, storage, installation, usage, renewal, revocation, backup and recovery of certificates/keys). As outlined in the Linking Technical Standards (LTS), only digital certificates issued by a Certificate Authority (CA) trusted by both Parties shall be used. The handling and storage of certificates/keys must follow the provisions set in the Handling Instructions.

Any revocation and/or renewal of certificates and keys shall be coordinated by both Parties. This takes place according to the Request Fulfilment procedures.

The Swiss registry administrator and the Union central administrator will exchange certificates/keys via secure means of communication according to the provisions laid down in the Handling Instructions.

Any verification of certificates/keys in any means between the Parties will take place out of band.

**DECISION No 2/2020 OF THE JOINT COMMITTEE ESTABLISHED BY THE AGREEMENT
BETWEEN THE EUROPEAN UNION AND THE SWISS CONFEDERATION ON THE LINKING OF
THEIR GREENHOUSE GAS EMISSIONS TRADING SYSTEMS**

of 5 November 2020

**on amending Annexes I and II to the Agreement and the adoption of Linking Technical Standards
(LTS) (2021/1034)**

THE JOINT COMMITTEE,

Having regard to the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems ⁽¹⁾ ('the Agreement') and in particular Article 3(7) and Article 13(2) thereof,

Whereas:

- (1) Decision No 2/2019 of the Joint Committee of 5 December 2019 ⁽²⁾ amended Annexes I and II to the Agreement thus fulfilling the conditions for linking set out in the Agreement.
- (2) Following adoption of Decision No 2/2019 of the Joint Committee and pursuant to Article 21(3) of the Agreement, the Parties exchanged their instruments of ratification or approval, since they consider all conditions for linking as set out in the Agreement to have been fulfilled.
- (3) In accordance with Article 21(4) of the Agreement, the Agreement entered into force on 1 January 2020.
- (4) Annex I to the Agreement should be amended in accordance with Article 13(2) of the Agreement to ensure a smooth transition in administration of aircraft operators attributed to Switzerland for the first time by taking account of the progress made on establishing the registry link.
- (5) In order to accommodate recent developments and ensure an increased level of flexibility to establish the registry link required by the Agreement, Annex II to the Agreement should be amended in accordance with Article 13(2) of the Agreement to provide for a larger, but equivalent set of technologies to set up the registry link.
- (6) Pursuant to Article 3(7) of the Agreement, the Swiss registry administrator and the Union central administrator should develop Linking Technical Standards (LTS) based on the principles set out in Annex II of the Agreement. The LTS should describe the detailed requirements for establishing a robust and secure connection between the Swiss Supplementary Transaction Log (SSTL) and the European Union Transaction Log (EUTL). The LTS should take effect when adopted by decision of the Joint Committee.
- (7) In accordance with Article 13(1) of the Agreement, the Joint Committee should agree on technical guidelines to ensure the proper implementation of the Agreement including on establishing a robust and secure connection between the SSTL and the EUTL. Technical guidelines may be developed by a working group set up pursuant to Article 12(5) of the Agreement. The working group should at least include the Swiss registry administrator and the Union central administrator and should assist the Joint Committee in its functions under Article 13 of the Agreement.
- (8) In view of the technical nature of the guidelines and the need to adapt them to ongoing developments, the technical guidelines developed by the Swiss registry administrator and the Union central administrator should be submitted to the Joint Committee for information or, where appropriate, approval,

⁽¹⁾ OJ L 322, 7.12.2017, p. 3.

⁽²⁾ Decision no 2/2019 of the Joint Committee established by the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 5 December 2019 amending Annexes I and II to the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems (OJ L 314, 29.9.2020, p. 68).

HAS ADOPTED THIS DECISION:

Article 1

The second paragraph of point 17 in Part B of Annex I to the Agreement is hereby replaced by the following text:

‘Aircraft operators attributed to Switzerland for the first time after the entry into force of this Agreement shall be administered by Switzerland after 30 April of the year of attribution and once the provisional registry link is operational.’.

Article 2

The fourth subparagraph of Annex II to the Agreement is hereby replaced by the following text:

‘The LTS shall specify that the communications between the SSTL and the EUTL consist of secure exchanges of webservices messages based on the following technologies (*) or equivalent:

- web services using Simple Object Access Protocol (SOAP);
- hardware-based Virtual Private Network (VPN);
- XML (Extensible Markup Language);
- digital signature; and
- network time protocols.

(*) Those technologies are currently used for establishing a connection between the Union Registry and the International Transaction Log as well as between the Swiss Registry and the International Transaction Log.’

Article 3

The Linking Technical Standards (LTS), as annexed to this Decision, are hereby adopted.

Article 4

Herewith, a working group shall be set up pursuant to Article 12(5) of the Agreement. It shall assist the Joint Committee in ensuring the proper implementation of the Agreement including the development of technical guidelines for the implementation of the LTS.

The working group shall at least include the Swiss registry administrator and the Union central administrator.

Article 5

This Decision shall enter into force on the day of its adoption.

Done at Brussels, 5 November 2020.

For the Joint Committee
Secretary for the European Union
Maja-Alexandra DITTEL

The Chair
Beatriz YORDI

Secretary for Switzerland
Caroline BAUMANN

ANNEX

Linking technical standards (LTS) pursuant to Article 3(7) of the Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems

STANDARDS FOR PROVISIONAL SOLUTION

1. **Glossary**

Table 1-1

Business Acronyms and Definitions

Acronym/Term	Definition
Allowance	An allowance to emit one tonne of carbon dioxide equivalent during a specified period, which shall be valid only for the purposes of meeting the requirements under the EU ETS or the ETS of Switzerland.
CH	Swiss Confederation
CHU	Swiss general allowances (Term 'CHU2' is used as abbreviation for commitment period 2 CHU allowances)
CHUA	Swiss Aviation Allowance
COP	Common Operational Procedures jointly developed by the Parties to the Agreement to operationalise the link between the EU ETS and the ETS of Switzerland.
ETR	Emissions Trading Registry
ETS	Emissions Trading System
EU	European Union
EUA	EU General Allowance
EUAA	EU Aviation Allowance
EUCR	European Union Consolidated Registry
EUTL	European Union Transaction Log
Registry	An accounting system for allowances issued under the ETS, which keeps track of the ownership of allowances held in electronic accounts.
SSTL	Swiss Supplementary Transaction Log
Transaction	A process in a registry that includes the transfer of an allowance from one account to another account.
Transaction log system	The transaction log contains a record of each proposed transaction sent from one Registry to the other.

Table 1-2

Technical Acronyms and Definitions

Acronym	Definition
Asymmetric cryptography	Uses public and private keys to encrypt and decrypt data.
Certificate Authority (CA)	Entity that issues digital certificates.

Acronym	Definition
Cryptographic key	A piece of information that determines the functional output of a cryptographic algorithm.
Decryption	Reverse process of encryption.
Digital signature	A mathematical technique used to validate the authenticity and integrity of a message, software or digital document.
Encryption	The process of converting information or data into a code, especially to prevent unauthorized access.
File ingestion	The process of reading a file.
Firewall	Network security appliance or software that monitors and controls incoming and outgoing network traffic based on predetermined rules.
Heartbeat monitoring	Periodic signal generated and monitored by hardware or software to indicate normal operation or to synchronize other parts of a computer system.
IPSec	IP SECurity. Network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network.
Penetration testing	Practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.
Reconciliation process	Process of ensuring that two sets of records are in agreement.
VPN	Virtual Private Network.
XML	Extensible Mark-up Language. It allows designers to create their own customised tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organisations.

2. Introduction

The Agreement between the European Union and the Swiss Confederation on the linking of their greenhouse gas emissions trading systems of 23 November 2017 ('Agreement') provides for the mutual recognition of emission allowances that can be used for compliance under the Emissions Trading System of the European Union ('EU ETS') or the Emissions Trading System of Switzerland ('ETS of Switzerland'). To operationalise the link between the EU ETS and the ETS of Switzerland, a direct link between the European Union Transaction Log (EUTL) of the Union Registry and the Swiss Supplementary Transaction Log (SSTL) of the Swiss registry will be established, which will enable the registry-to-registry transfer of emission allowances issued under either ETS (Article 3(2) of the Agreement). To operationalise the link between the EU ETS and the ETS of Switzerland, a provisional solution shall be in place by May 2020 or as soon as possible thereafter. Parties shall cooperate to replace the provisional solution with a permanent registry link as soon as possible (Annex II to the Agreement).

Pursuant to Article 3(7) of the Agreement, the Swiss registry administrator and the Union central administrator shall develop Linking Technical Standards (LTS) based on the principles set out in Annex II to the Agreement, describing the detailed requirements for establishing a robust and secure connection between the SSTL and the EUTL. The LTS developed by the administrators shall take effect when adopted by a decision of the Joint Committee.

The LTS, as recorded in this document is to be adopted by the Joint Committee by its Decision No 2/2020. In accordance with this Decision, the Joint Committee shall request the Swiss registry administrator and the Union central administrator to develop further technical guidelines to operationalise the link and to ensure that these are continuously adapted to technical progress and new requirements relating to the safety and security of the link and to its effective and efficient operation.

2.1. *Scope*

This document represents the common understanding between the Parties to the Agreement regarding the establishment of the technical foundations of the link between the registries of the EU ETS and the ETS of Switzerland. While it outlines the baseline for the technical specifications in terms of architectural, service and security requirements, some further detailed guidance will be needed to operationalise the link.

For its proper functioning, the link will require processes and procedures in order to further operationalise it. Pursuant to Article 3(6) of the Agreement, those matters are detailed in a separate common operational procedures (COP) document, to be adopted separately by decision of the Joint Committee.

2.2. *Addressees*

This document is addressed to the Swiss registry administrator and the Union central administrator.

3. **General provisions**

3.1. *Architecture of the Communication Link*

The purpose of this section is to provide a description of the general architecture of the operationalisation of the link between the EU ETS and the ETS of Switzerland and the different components involved in it.

Security being a key part of the definition of the architecture of the registry link, all measures have been taken to have a robust architecture. Although the foreseen permanent registry link will be based on web services, the provisional solution will use a file exchange mechanism instead.

The technical solution uses:

- A secure message exchange transfer protocol;
- XML messages;
- XML based digital signature and encryption;
- VPN Appliance or equivalent secure data transport network.

3.1.1. *Message Exchange*

The communication between the Union Registry and the Swiss registry will be based on a message exchange mechanism through secured channels. Each end will count on its own repository of received messages.

Both Parties will keep a log of the messages received, together with the processing details.

Errors or an unexpected status are to be reported as alerts and human contact between the support teams should take place.

Errors and unexpected events will be handled in observance of the operational procedures laid down in the incident management process of the COP.

3.1.2. *XML Message – High level Description*

An XML Message contains one of the following:

- One or several Transaction Requests and/or one or several Transaction Responses;
- One operation/response related to reconciliation;
- One Test message.

Every message contains a header with:

- Originating ETS system;
- Sequence Number.

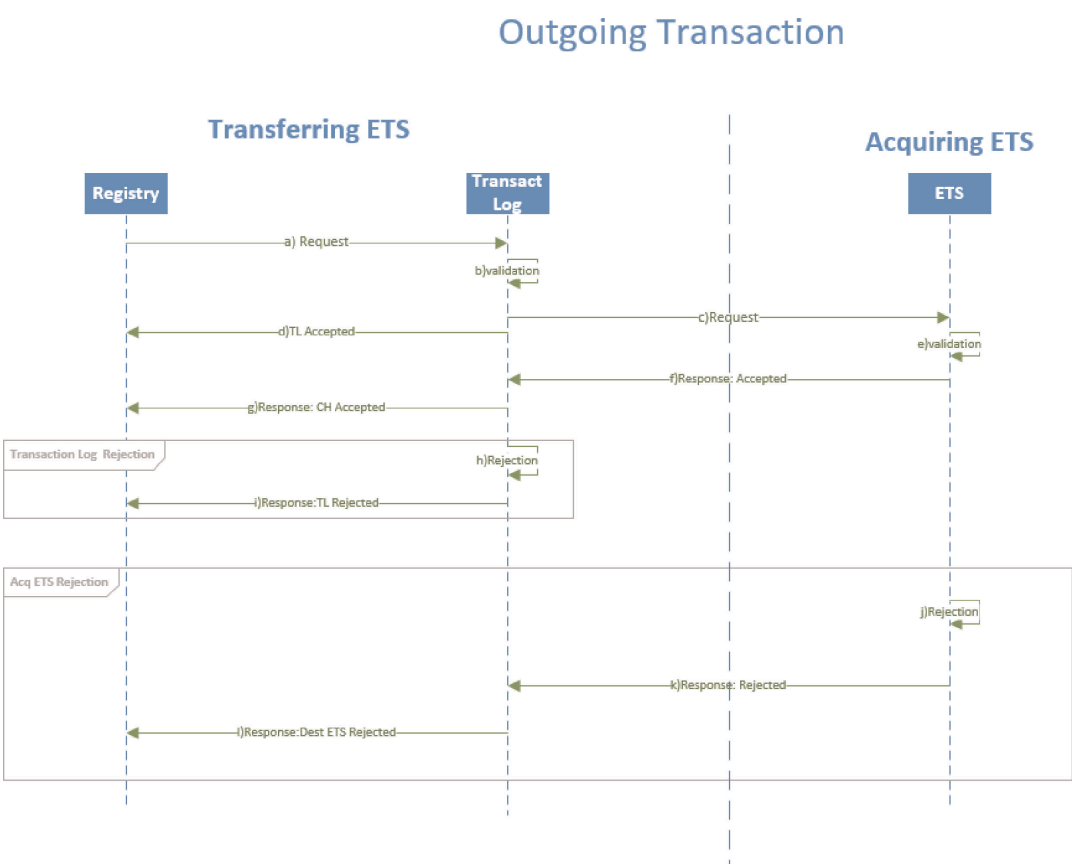
3.1.3. Ingestion windows

The provisional solution is based on predefined ingestion windows that are followed by a set of named events. Transaction requests received through the link will only be ingested at predefined intervals. Ingestion windows include a technical validation for outgoing and incoming transactions. In addition, reconciliations may run on a daily basis and can be triggered manually.

Changes in the frequency and/or timing of any of these events will be handled in observance of the operational procedures laid down in the request fulfilment process of the COP.

3.1.4. Transaction Message Flows

Outgoing transactions



This reflects the point of view of the transferring ETS. The sequence diagram above depicts all the specific outgoing transaction flows.

Main flow 'Normal Transaction' (with steps indicated in the drawing above):

- On the transferring ETS, the transaction request is sent from the registry to the Transaction log, once all the business delays are over (24 hours delay, where applicable);
- Transaction log validates the transaction request;
- The transaction request is sent to the destination ETS;
- The acceptance response is sent to the originating ETS registry;

- (e) The destination ETS validates the transaction request;
- (f) The destination ETS sends the acceptance response back to the originating ETS Transaction log;
- (g) The Transaction log sends the acceptance response to the registry.

Alternative flow 'Transaction Log Rejection' (with steps indicated in the drawing above, starting equally from (a)):

- (a) In the originating ETS, the transaction request is sent from the registry to the Transaction log, once all the business delays are over (24 hours delay, where applicable).

Followed by:

- (b) Transaction log does not validate the request;
- (c) Rejection message is sent to the originating registry.

Alternative flow 'ETS Rejection' (with steps indicated in the drawing above, starting from (a)):

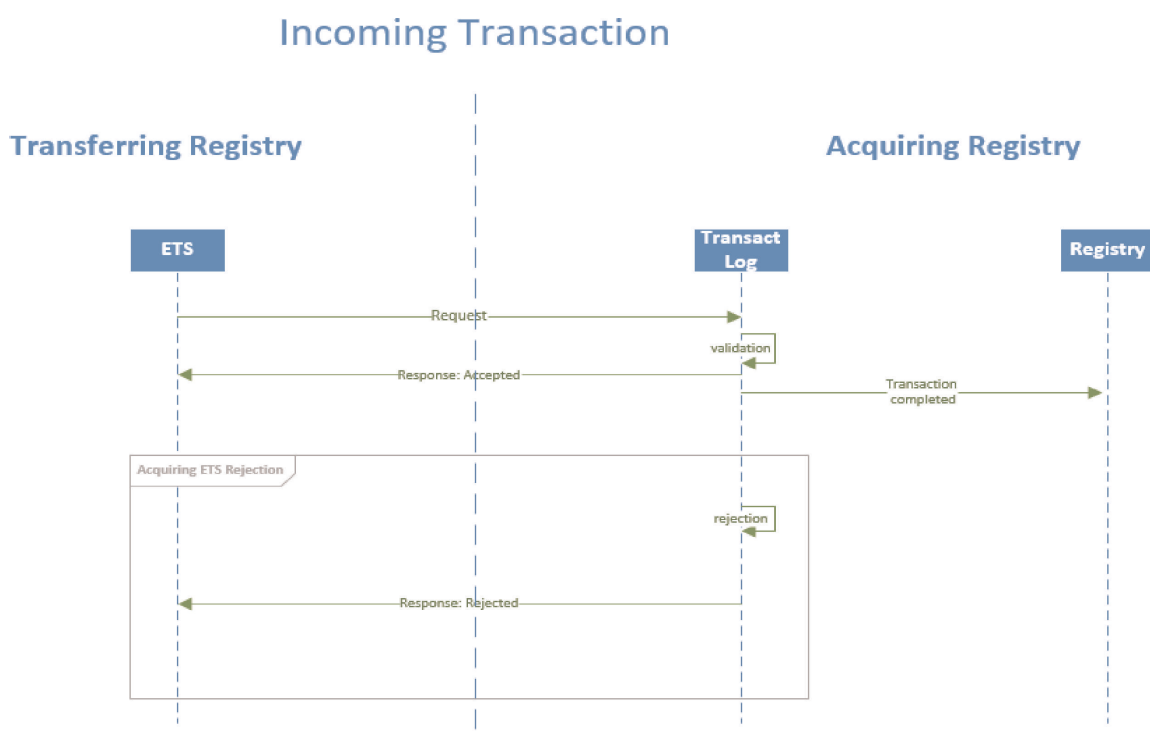
- (a) In the originating ETS, the transaction request is sent from the registry to the Transaction log, once all business delays are over (24 hours delay, where applicable);
- (b) Transaction log validates the transaction;
- (c) The transaction request is sent to the destination ETS;
- (d) The acceptance message is sent to the originating ETS registry.

Followed by:

- (e) The acquiring ETS Transaction log does not validate the transaction;
- (f) Acquiring ETS sends the refusal response to the transferring ETS Transaction log;
- (g) Transaction log send the refusal to the registry.

Incoming Transactions

This reflects the point of view of the acquiring ETS. The specific flow is depicted in the following sequence diagram:



The diagram shows:

1. When the acquiring ETS Transaction log validates the request, it sends the acceptance message to the Transferring ETS and a 'transaction completed' message to the acquiring ETS registry;
2. When an incoming request is refused on the acquiring Transaction log and it is refused, the transaction request is not sent to the acquiring ETS registry.

Protocol

The transaction message cycle involves only two messages:

- Transferring ETS → Acquiring ETS Transaction Proposal;
- Acquiring ETS → Transferring ETS Transaction Response: Either Accepted or Rejected (including the reason for rejection):
 - Accepted: Transaction is completed;
 - Rejected: Transaction is terminated.

Transaction status

- Transferring ETS transaction status will be set to 'proposed' when the request is sent.
- Acquiring ETS transaction status will be set to 'proposed' when the request is received and while it is being treated.
- Acquiring ETS transaction status will be set to 'completed'/'terminated', when the proposal is processed. Acquiring ETS will then send the corresponding acceptance/rejection message.
- Transferring ETS transaction status will be set to 'completed'/'terminated' when the acceptance/rejection is received and processed.
- In the Transferring ETS the transaction status will remain as proposed if no response is received.
- Acquiring ETS transaction status will be set to 'terminated' if any proposed transaction stays in the 'proposed' state for more than 30 minutes.

Incidents related to transactions will be handled in observance of the operational procedures laid down in the incident management process of the COP.

3.2. Data Transfer Security

The data in transit will be subject to four levels of security:

- (1) Network access control: Firewall and network interconnection layer;
- (2) Transport level encryption: VPN or equivalent secure data transport network;
- (3) Session level encryption: Secure message exchange transfer protocol;
- (4) Application level encryption: XML Content encryption and signature.

3.2.1. Firewall and Network Interconnection

The link shall be established over a network protected by a hardware-based firewall. The firewall shall be configured with rules such that only 'registered' clients can make connections to the VPN server.

3.2.2. Virtual Private Network (VPN)

All communications between the Parties shall be protected using a secure data transport technology. In the case of a Virtual Private Network (VPN), the infrastructure should be based on hardware or virtual appliances. VPN technologies provide the ability to 'tunnel' through a network like the Internet from one point to another, protecting all communications. Prior to the creation of the VPN tunnel, a digital certificate is issued to a prospective client end-point, allowing the client to provide proof of identity during the negotiation of the connection. Each Party is responsible for installing the certificate into its VPN end-point. Using digital certificates, each end VPN server will access a central authority to negotiate authentication credentials. During the tunnel creation process, encryption is negotiated, ensuring that all communications through the tunnel are protected.

The client VPN end-points shall be configured to maintain the VPN tunnel permanently, in order to allow reliable, two-way, real-time communication between the Parties at all times.

Any other equivalent solution shall be compliant with the abovementioned principles.

3.2.3. IPSec Implementation

In case of using a VPN solution, the use of the IPSec protocol to form the site-to-site VPN infrastructure will provide for site-to-site authentication, data integrity, and data encryption. IPSec VPN configurations ensure proper authentication between two end-points in a VPN connection. The Parties will identify and authenticate the remote client via the IPSec connection using a digital certificates provided by a Certificate Authority recognised by the other end.

IPSec also ensures data integrity of all communications passed through the VPN tunnel. Data packets are hashed and signed using the authentication information established by the VPN. Confidentiality of the data is assured likewise by enabling IPSec encryption.

3.2.4. Secure Message Exchange Transfer Protocol

The provisional solution relies on multiple encryption layers to securely exchange data between the Parties. Both systems and their different environments are interconnected at the network level by means of VPN tunnels or equivalent secure data transport networks. At the application level files are transferred using a secure message exchange transfer protocol at session level.

3.2.5. XML Encryption and Signature

Within XML files, signing and encryption occurs at two levels. Every transaction request, transaction response and reconciliation message is digitally signed individually.

In a second step, every sub element of the 'message' element is individually encrypted.

In addition, as a third step and to ensure the integrity and non-repudiation of the whole message, the root element message is digitally signed. This results in a high level of protection for the XML embedded data. The technical implementation observes the World Wide Web Consortium standards.

To decrypt and verify the message, the process is followed in reverse order.

3.2.6. Cryptographic Keys

Public key cryptography will be used for encryption and signing.

For the specific case of IPSec, a digital certificate issued by a Certificate Authority (CA) trusted by both Parties shall be used. This CA verifies the identity of the certificate holder and issues certificates which are used to positively identify an organisation and set up secure data communications channels between the Parties.

Cryptographic keys are used for signing and encrypting communication channels and data files. The public certificates are digitally exchanged by the Parties using secure channels and verified out of band. This procedure is an integral part of the Information Security Management process of the COP.

3.3. *List of Functions under the Link*

The link specifies the transmission system for a series of functions that implement the business processes derived from the Agreement. The link also includes the specification for the reconciliation process and for the test messages that will allow the implementation of heartbeat monitoring.

3.3.1. Business Transactions

From the business perspective, the link contemplates four (4) types of Transaction Requests:

— External transfer:

— After entry into force of the ETS linking, EU and CH allowances are fungible, and thus fully transferrable, between the Parties;

- A transfer sent through the link will involve a transferring account on an ETS and acquiring account on the other ETS;
- The transfer can include any amount of the four (4) types of allowances:
 - Swiss general allowances (CHU);
 - Swiss aviation allowances (CHUA);
 - EU general allowances (EUA);
 - EU aviation allowances (EUAA).
- International Allocation:

Aircraft Operators administered by one ETS with obligations on the other ETS and entitled to receive free allowances from that second ETS, will receive free aviation allowances, from the second ETS, by means of the international allocation transaction.
- Reversal of International Allocation:

This transaction will happen in the case that free allowances allocated to an aircraft operator holding by the other ETS have to be reversed in total.
- Return of Excess Allocation:

Similar to the reversal, but where the allocation does not need to be fully reversed, and only the over-allocated allowances have to be returned to the allocating ETS.

3.3.2. Reconciliation Protocol

Reconciliations will only take place after the windows for messages ingestion, validation and processing are closed.

Reconciliations are an integral part of the security and consistency measures of the linking. Both Parties will agree on the exact timing of reconciliation before creating any schedule. A daily scheduled reconciliation can take place if agreed by both Parties. At a minimum, at least one scheduled reconciliation will be executed after each ingestion takes place.

In any case, either Party can initiate manual reconciliations at any time.

Changes in the timing and frequency of the scheduled reconciliation will be handled in observance of the operational procedures laid down in the request fulfilment process of the COP.

3.3.3. Test Message

A test message is provided for to test end-to-end communication. The message will contain data that will identify the message as a test and will be answered upon reception by the other end.

3.4. *Standards for Web Services*

Web services will not be used in the provisional solution. It is worth noting however that the shape and format of XML messages will remain unchanged to a great extent. With the introduction of the permanent registry link in the future, web services should allow the exchange of XML messages in real-time.

3.5. *Web Services Specific Definition*

This section is not applicable for the provisional solution. As mentioned in the previous section, web services will only be used in the future permanent registry link.

3.6. *Data Logging Requirements*

To support the need for both Parties to maintain accurate and consistent information, and to provide tools for use in the reconciliation process to resolve inconsistencies, four (4) types of data logs shall be maintained by both Parties:

- Transaction logs;
- Reconciliation logs;

- Message archive;
- Internal audit logs.

All data in these logs shall be maintained at least during three (3) months for the purposes of troubleshooting and their further retention will depend on the applicable law at each end for the purpose of auditing. Log files older than three (3) months may be archived into a secure location in an independent IT system, as long as they can be retrieved or accessed within a reasonable period.

Transaction Logs

Both EUTL and SSTL subsystems contain Transaction log implementations.

More specifically, the Transaction logs will keep a record of each proposed transaction sent to the other ETS. Each record contains all the fields of the transaction content and the subsequent outcome of the transaction (the response of the receiving ETS). The Transaction logs will also keep a record for the incoming transactions as well as the response sent to the originating ETS.

Reconciliation Logs

The Reconciliation Log contains a record of each reconciliation message exchanged between both Parties, including the reconciliation id, the timestamp and the result of the reconciliation: Reconciliation status 'Pass' or 'Discrepancies'. In the provisional solution reconciliation messages are an integral part of the messages exchanged.

Both Parties shall log each request and its response in the Reconciliation Log. Although information in the Reconciliation Log is not shared directly as part of the Reconciliation itself, access to this information may be necessary in order to resolve inconsistencies.

Message Archive

Both Parties are required to archive a copy of the exchanged data (the XML files), sent and received, and whether those or XML messages were correct in their format or not.

The main purpose of the archive is for auditing, to have evidence of what was sent and received to and from the other Party. In that sense, along with the files, the related certificates need to be archived as well.

These files will also provide additional information for troubleshooting.

Internal Audit Log

These logs are defined and used by each Party on its own.

3.7. Operational Requirements

The exchange of data between both systems is not fully autonomous in the provisional solution, this means it requires operators and procedures to operationalise the link.

4. Availability provisions

4.1. Communication Availability Design

The architecture for the provisional solution is fundamentally an ICT infrastructure and software that allows the communication between the ETS of Switzerland and the EU ETS. Ensuring high levels of availability, integrity and confidentiality of this flow of data therefore becomes an essential aspect to consider in the design of the provisional solution and the permanent registry link. Being a project in which the ICT infrastructure, the custom made software, and the processes play an integral role, all three elements have to be taken into account in order to design a resilient system.

ICT infrastructure resilience

The general provisions chapter of this document details the architectural building blocks. On the ICT infrastructure side, the provisional linking sets up a resilient VPN network (or equivalent) that creates secure communication tunnels over which secure message exchanges can take place. Other infrastructure elements are configured in high-availability and/or count on fall-back mechanisms.

Custom Software resilience

The custom developed software modules enhance the resilience by retrying the communication for a given period of time with the other end if due to any reason, it is not available.

Service resilience

In the provisional solution, data exchanges between Parties occur at predefined timeslots throughout the year. Some of the steps required in the prescheduled data exchanges require manual intervention by system operators and/or registry administrators. Taking this aspect into account, and in order to increase the availability and success of the exchanges:

- The operational procedures foresee significant time windows to perform each step;
- The software modules for the provisional solution implement asynchronous communication;
- The automatic reconciliation process will detect if there were issues in the ingestion of data files at either end;
- Monitoring processes (ICT infrastructure and custom software modules) are considered in, and trigger, Incident Management procedures (as defined in the common operational procedures document). Those procedures that aim at reducing the time to restore normal operation following incidents are essential to ensure high availability ratios.

4.2. *Initialisation, Communication, Re-activation and Testing Plan*

All different elements involved in the architecture of the provisional solution shall pass a series of individual and collective tests in order to confirm the platform is ready at ICT infrastructure and information system level. These operational tests are a compulsory prerequisite each time the platform transitions the provisional solution from suspended to operational status.

The operational status activation of the link requires then the successful execution of a predefined test plan. This shall confirm that each registry has performed a set of internal test first, followed by end-to-end connectivity validation prior to beginning the submission of production transactions between both Parties.

The test plan should mention the overall test strategy and details about the testing infrastructure. In particular, for each element in every test block it should include:

- The test criteria and tools;
- The roles assigned to perform the test;
- The expected results (positive and negative);
- Test schedule;
- The logging of test results requirements;
- Troubleshooting documentation;
- Escalation provisions.

As a process, the operational status activation tests could be split into four (4) conceptual blocks or phases:

4.2.1. Internal ICT Infrastructure Tests

These tests are meant to be performed and/or checked individually by both Parties at each end.

Every element of ICT infrastructure at each end shall be tested individually. This includes every single component of the infrastructure. These tests can be executed automatically or manually but shall verify that every element of the infrastructure is operational.

4.2.2. Communication Tests

These tests are triggered individually by either Party and concluding the tests requires the cooperation of the other end.

Once individual elements are operational, the communication channels between both registries needs to be tested. To this end, each Party shall verify that Internet access works, the VPN tunnels (or equivalent secure transport network) are established, and there is site-to-site IP connectivity. Reachability of the local and remote infrastructure elements and IP connectivity should then be confirmed at the other end.

4.2.3. Full System (end-to-end) Tests

These tests are meant to be executed at each end and results shall be shared with the other Party.

Once communication channels and each individual component of both registries have been tested, each end shall prepare a series of simulated transactions and reconciliation that are representative of all functions to be implemented under the link.

4.2.4. Security Tests

These tests are meant to be performed and/or triggered by both Parties at each end and as detailed in sections 5.4, 'Security Testing Guidelines', and 5.5, 'Risk Assessment Provisions'.

Only after each of the four phases/blocks have ended with a predictable results can the provisional link be considered in operational status.

Testing resources

Each Party shall count on specific testing resources (specific ICT infrastructure software and hardware) and shall develop testing functions in their respective systems in order to support the manual and continuous validation of the platform. Manual individual or cooperative testing procedures can be executed at any time by registry administrators. Operational status activation is a manual process in itself.

It is likewise provided for that the platform performs automatic checks at regular intervals. Those checks are aimed at increasing the availability of the platform by detecting early potential infrastructure or software issues. This platform monitoring plan is composed of two elements:

- ICT infrastructures monitoring: at both ends the infrastructure will be monitored by the ICT infrastructure service providers. The automatic tests will cover the different infrastructure elements and the availability of communication channels.
- Application monitoring: the provisional linking software modules will implement system communication monitoring at application level (either manually and/or at regular intervals) that will test the end-to-end availability of the linking by simulating some of the transactions over the link.

4.3. *Acceptance/Testing Environments*

The architecture of the Union Registry and the registry of Switzerland consist of the following three environments:

- Production (PROD): This environment holds the real data and processes real transactions;
- Acceptance (ACC): This environment contains non-real or anonymised, representative data. It is the environment where system operators by both Parties validate new releases;
- Test (TEST): This environment contains non-real or anonymised, representative data. This environment is limited to registry administrators and is meant to be used to perform integration tests by both Parties.

Except for the VPN (or equivalent network), the three environments are fully independent of each other, meaning hardware, software, databases, virtual environments, IP-addresses and ports are set up and operate independently of each other.

As for the VPN layout, this is set up in two different environments, one for PROD, another independent one for ACC and TEST.

5. **Confidentiality and integrity provisions**

Security Mechanisms and Procedures provide for a two-person method (4-eye principle) for operations occurring in the link between the Union Registry and the Swiss registry. The two-person method shall apply whenever necessary. However, it might not apply to all steps undertaken by registry administrators.

The security requirements are considered and addressed in the security management plan, which also includes processes related to the handling of security incidents following an eventual security breach. The operational part of these processes is described in the COP.

5.1. *Security Testing Infrastructure*

Each Party commits to setting up a security testing infrastructure (by using the common set software and hardware used in the detection of vulnerabilities at development and operation phases):

- Separated from the production environment;
- Where security is analysed by a team independent from the development and the operation of the system.

Each Party commits to performing both static and dynamic analysis.

In the case of dynamic analysis (like penetration testing), both Parties commit to restricting the evaluations ordinarily to the test and acceptance environments (as defined in section 4.3, 'Acceptance/Testing environments'). Exceptions to this policy are subject to the approval of both Parties.

Before being deployed in the production environment, every software module of the link (as defined in section 3.1, 'Architecture of the communication link') shall be security tested.

Testing infrastructure must be separated at both network and infrastructure levels from the production infrastructure. The security tests required to check compliance with security requirements are carried out within the testing infrastructure.

5.2. *Link Suspension and Reactivation Provisions*

Where there is a suspicion that the security of the registry of Switzerland, the SSTL, the Union registry or the EUTL has been compromised, either Party shall immediately inform the other and suspend the link between the SSTL and the EUTL.

The procedures for information sharing, for a decision to suspend and for a decision to reactivate are part of the Request Fulfilment process of the COP.

Suspensions

Suspension of the registry link in accordance with the Annex II of the Agreement may happen due to:

- Administrative reasons (for example, maintenance), which are planned;
- Security reasons (or IT infrastructure breakdowns), which are unplanned.

In case of an emergency, either Party will inform the other Party and suspend unilaterally the registry link.

If the decision is made to suspend the registry link, each Party will therefore ensure that the link is interrupted at network level (by blocking parts or all of incoming and outgoing connections).

The decision to suspend the registry link, whether it is planned or unplanned, will be taken in accordance with the Change Management or Security Incident Management procedure of the COP.

Communication Reactivation

A decision to reactivate the registry link will be taken in the manner detailed in the COP and in any case not before the successful completion of the security testing procedures as detailed in sections 5.4, 'Security testing guidelines', and 4.2, 'Initialisation, Communication, Re-activation and Testing Plan'.

5.3. *Security Breach Provisions*

A security breach is considered to be a Security Incident impacting the confidentiality and the integrity of any sensitive information and/or the availability of the system handling them.

Sensitive information is identified in the Sensitive Information List and may be handled in the system or in any related part of the system.

Information directly related to the security breach will be considered to be sensitive, marked 'ETS CRITICAL' and handled in accordance with the handling instructions, unless specified otherwise.

Every security breach will be handled in accordance with the Security Incident Management chapter of the COP.

5.4. *Security Testing Guidelines*

5.4.1. Software

Security testing, including penetration testing, if applicable, shall be performed at least on all new major releases of the software in accordance with the security requirements set out in the LTS in order to assess the security of the linking and the related risks.

If no major release has been produced in the last 12 months, security testing shall be performed on the current system, taking into account the cyber threat evolution that occurred in the last 12 months.

Security testing of the registry link shall be done in the acceptance environment and, if required, in the production environment and with the coordination and mutual agreement of both Parties.

Web application testing will observe international open standards such as the ones developed by the Open Web Application Security Project (OWASP).

5.4.2. Infrastructure

The infrastructure supporting the production system shall be regularly scanned against vulnerabilities (at least once a month) and detected vulnerabilities shall be fixed. Testing is performed according to the method outlined in section 5.4.1, using an up-to-date vulnerability database.

5.5. *Risk Assessment Provisions*

If penetration testing is applicable it must be included in the security testing.

Each Party may contract a specialized company for the performance of security testing, provided this company:

- Has the skills and the experience of such security testing;
 - Is not reporting directly to the developer and/or its contractor and is neither involved in the development of the software of the link nor a subcontractor of the developer;
 - Has signed Non-Disclosure Agreement to keep the results confidential and to handle them at the 'ETS CRITICAL' level in accordance with handling instructions.
-

COMMISSION IMPLEMENTING DECISION (EU) 2021/1035**of 23 June 2021****amending Implementing Decisions 2013/648/EU and 2013/650/EU as regards the authorisation holder and its representative in the Union for the placing on the market of products containing, consisting of, or produced from certain genetically modified maize***(notified under document C(2021) 4317)***(Text with EEA relevance)****(Only the Dutch text is authentic)**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EC) No 1829/2003 of the European Parliament and of the Council of 22 September 2003 on genetically modified food and feed ⁽¹⁾, and in particular to Articles 9(2) and 21(2) thereof,

Whereas:

- (1) Bayer Agriculture BVBA, based in Belgium, is the representative in the Union of Monsanto Company, based in the United States of America, concerning the authorisations for the placing on the market of products containing, consisting of, or produced from genetically modified maize authorised by Commission Implementing Decisions 2013/648/EU ⁽²⁾ and 2013/650/EU ⁽³⁾. Dow AgroSciences LLC, based in the United States of America, is the other authorisation holder for the genetically modified maize authorised by these Implementing Decisions. Dow AgroSciences LLC is represented by Dow AgroSciences Distribution S.A.S., based in France.
- (2) By letter dated 28 July 2020, Bayer Agriculture BVBA, based in Belgium, informed the Commission that Monsanto Company, based in the United States, converts its legal form and changes its name to Bayer CropScience LP, based in the United States of America, as of 1 August 2020.
- (3) By letter dated 28 July 2020, Bayer Agriculture BVBA, informed the Commission that it changes its name to Bayer Agriculture BV, based in Belgium, as of 1 August 2020.
- (4) By the letter dated 17 March 2021, the Commission was informed that Dow AgroSciences LLC changed the name to Corteva Agriscience LLC, based in the United States of America, as of 1 January 2021.
- (5) By the letter dated 22 March 2021, Corteva Agriscience LLC informed the Commission that its representative in the Union is Corteva Agriscience Belgium B.V., as of 22 March 2021.
- (6) The requested changes are purely administrative in nature and therefore do not entail a new assessment of the products concerned.

⁽¹⁾ OJ L 268, 18.10.2003, p. 1.

⁽²⁾ Commission Implementing Decision 2013/648/EU of 6 November 2013 authorising the placing on the market of products containing, consisting of, or produced from genetically modified maize MON89034 × 1507 × NK603 (MON-89034-3 × DAS-Ø15Ø7-1 × MON-ØØ6Ø3-6) pursuant to Regulation (EC) No 1829/2003 of the European Parliament and of the Council (OJ L 302, 13.11.2013, p. 38).

⁽³⁾ Commission Implementing Decision 2013/650/EU of 6 November 2013 authorising the placing on the market of products containing, consisting of, or produced from genetically modified (GM) maize MON 89034 × 1507 × MON88017 × 59122 (MON-89034-3 × DAS-Ø15Ø7-1 × MON-88Ø17-3 × DAS-59122-7), four related GM maizes combining three different single GM events (MON89034 × 1507 × MON88017 (MON-89Ø34-3 × DAS-Ø15Ø7-1 × MON-88Ø17-3), MON89034 × 1507 × 59122 (MON-89Ø34-3 × DAS-Ø15Ø7-1 × DAS-59122-7), MON89034 × MON88017 × 59122 (MON-89Ø34-3 × MON-88Ø17-3 × DAS-59122-7), 1507 × MON 88017 × 59122 (DAS-Ø15Ø7-1 × MON-88Ø17-3 × DAS-59122-7)) and four related GM maizes combining two different single GM events (MON89034 × 1507 (MON-89Ø34-3 × DAS-Ø15Ø7-1), MON89034 × 59122 (MON-89Ø34-3 × DAS-59122-7), 1507 × MON88017 (DAS-Ø15Ø7-1 × MON-88Ø17-3), MON 88017 × 59122 (MON-88Ø17-3 × DAS-59122-7)) pursuant to Regulation (EC) No 1829/2003 of the European Parliament and of the Council (OJ L 302, 13.11.2013, p. 47).

- (7) Implementing Decisions 2013/648/EU and 2013/650/EU should therefore be amended accordingly.
- (8) The measures provided for in this Decision are in accordance with the opinion of the Standing Committee on Plants, Animals, Food and Feed,

HAS ADOPTED THIS DECISION:

Article 1

Amendments to Implementing Decision 2013/648/EU

Implementing Decision 2013/648/EU is amended as follows:

- (1) in Article 6, paragraph 1 is replaced by the following:

‘1. The authorisation holders shall be:

- (a) Corteva Agriscience LLC, United States of America, represented by Corteva Agriscience Belgium B.V.; and
- (b) Bayer CropScience LP, United States of America, represented by Bayer Agriculture BV, Belgium.’;

- (2) Article 8 is replaced by the following:

‘This Decision is addressed to:

- (a) Corteva Agriscience LLC, 9330 Zionsville Road Indianapolis, Indiana 46268-1054, United States of America, represented by Corteva Agriscience Belgium B.V., Bedrijvenlaan 9, 2800 Mechelen, Belgium; and
- (b) Bayer CropScience LP, 800 N. Lindbergh Boulevard, St Louis, Missouri, 63167, United States of America, represented by Bayer Agriculture BV, Scheldelaan 460, 2040 Antwerp, Belgium.’;

- (3) in the Annex, point (a) is replaced by the following:

‘(a) **Applicants and Authorisation holders**

Name: Corteva Agriscience LLC

Address: 9330 Zionsville Road Indianapolis, Indiana 46268-1054, United States of America

represented by Corteva Agriscience Belgium B.V., Bedrijvenlaan 9, 2800 Mechelen, Belgium,
and

Name: Bayer CropScience LP

Address: 800 N. Lindbergh Boulevard, St Louis, Missouri, 63167, United States of America

represented by Bayer Agriculture BV, Scheldelaan 460, 2040 Antwerp, Belgium’.

Article 2

Amendments to Implementing Decision 2013/650/EU

Implementing Decision 2013/650/EU is amended as follows:

- (1) in Article 6, paragraph 1 is replaced by the following:

‘1. The authorisation holders shall be:

- (a) Corteva Agriscience LLC, United States of America, represented by Corteva Agriscience Belgium B.V.; and
- (b) Bayer CropScience LP, United States of America, represented by Bayer Agriculture BV, Belgium.’;

(2) Article 8 is replaced by the following:

‘This Decision is addressed to:

- (a) Corteva Agriscience LLC, 9330 Zionsville Road Indianapolis, Indiana 46268-1054, United States of America, represented by Corteva Agriscience Belgium B.V., Bedrijvenlaan 9, 2800 Mechelen, Belgium; and
- (b) Bayer CropScience LP, 800 N. Lindbergh Boulevard, St Louis, Missouri, 63167, United States of America, represented by Bayer Agriculture BV, Scheldelaan 460, 2040 Antwerp, Belgium.’;

(3) in the Annex, point (a) is replaced by the following:

‘(a) **Applicants and Authorisation holders**

Name: Corteva Agriscience LLC

Address: 9330 Zionsville Road Indianapolis, Indiana 46268-1054, United States of America

represented by Corteva Agriscience Belgium B.V., Bedrijvenlaan 9, 2800 Mechelen, Belgium
and

Name: Bayer CropScience LP

Address: 800 N. Lindbergh Boulevard, St Louis, Missouri, 63167, United States of America

represented by Bayer Agriculture BV, Scheldelaan 460, 2040 Antwerp, Belgium.’

Article 3

Addressees

This Decision is addressed to:

- (a) Corteva Agriscience LLC, 9330 Zionsville Road Indianapolis, Indiana 46268-1054, United States of America, represented by Corteva Agriscience Belgium B.V., Bedrijvenlaan 9, 2800 Mechelen, Belgium; and
- (b) Bayer CropScience LP, 800 N. Lindbergh Boulevard, St Louis, Missouri, 63167, United States of America, represented by Bayer Agriculture BV, Scheldelaan 460, 2040 Antwerp, Belgium.

Done at Brussels, 23 June 2021.

For the Commission
Stella KYRIAKIDES
Member of the Commission

COMMISSION IMPLEMENTING DECISION (EU) 2021/1036**of 22 June 2021****amending Implementing Decision (EU) 2018/1113 as regards the authorisation holder and its representative in the Union for the placing on the market of products produced from genetically modified sugar beet H7-1***(notified under document C(2021) 4325)***(Only the Dutch and German texts are authentic)****(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EC) No 1829/2003 of the European Parliament and of the Council of 22 September 2003 on genetically modified food and feed ⁽¹⁾, and in particular to Article 9(2) and Article 21(2) thereof,

Whereas:

- (1) Bayer Agriculture BVBA, based in Belgium, is the representative in the Union of Monsanto Company, based in the United States, concerning the authorisation for the placing on the market of products produced from genetically modified sugar beet H7-1 pursuant to Commission Implementing Decision (EU) 2018/1113 ⁽²⁾. KWS SAAT SE, based in Germany, is the authorisation holder for the genetically modified sugar beet H7-1, authorised by that Implementing Decision.
- (2) By letter dated 28 July 2020, Bayer Agriculture BVBA informed the Commission that it converts its legal form and changes its name to Bayer Agriculture BV as of 1 August 2020.
- (3) By letter dated 28 July 2020, Bayer Agriculture BVBA informed the Commission that Monsanto Company converts its legal form and changes its name to Bayer CropScience LP as of 1 August 2020.
- (4) The requested changes are purely administrative in nature and therefore do not entail a new assessment of the products concerned.
- (5) By letter dated 10 August 2020, the Commission informed KWS SAAT SE about the requested changes. By letter of 9 December 2020, KWS SAAT SE informed the Commission that it agrees with the proposed modifications.
- (6) Implementing Decision (EU) 2018/1113 should therefore be amended accordingly.
- (7) The measures provided for in this Decision are in accordance with the opinion of the Standing Committee on Plants, Animals, Food and Feed,

HAS ADOPTED THIS DECISION:

*Article 1***Amendments to Implementing Decision (EU) 2018/1113**

Implementing Decision (EU) 2018/1113 is amended as follows:

⁽¹⁾ OJ L 268, 18.10.2003, p. 1.

⁽²⁾ Commission Implementing Decision (EU) 2018/1113 of 3 August 2018 renewing the authorisation for the placing on the market of food and feed produced from genetically modified sugar beet H7-1 (KM-ØØØH71-4) pursuant to Regulation (EC) No 1829/2003 of the European Parliament and of the Council (OJ L 203, 10.8.2018, p. 32).

(1) in Article 6, paragraph 1, point (b) is replaced by the following:

‘(b) Bayer CropScience LP, represented in the Union by Bayer Agriculture BV;’

(2) in Article 8, point (b) is replaced by the following:

‘(b) Bayer CropScience LP, 800 N, Lindbergh Boulevard, St. Louis, Missouri 63167, United States of America, represented in the Union by Bayer Agriculture BV, Scheldelaan 460, 2040 Antwerp, Belgium.’;

(3) in the Annex, point (a) is replaced by the following:

‘(a) Applicants and authorisation holders:

Name: KWS SAAT SE

Address: Grimsehlstrasse 31, 37574 Einbeck, Germany

and

Name: Bayer CropScience LP

Address: 800 N, Lindbergh Boulevard, St. Louis, Missouri 63167, United States of America

Represented in the Union by Bayer Agriculture BV, Scheldelaan 460, 2040 Antwerp, Belgium.’

Article 2

Addressees

This Decision is addressed to:

(a) KWS SAAT SE, Grimsehlstrasse 31, 37574 Einbeck, Germany, and

(b) Bayer CropScience LP, 800 N, Lindbergh Boulevard, St. Louis, Missouri 63167, United States of America, represented in the Union by Bayer Agriculture BV, Scheldelaan 460, 2040 Antwerp, Belgium.

Done at Brussels, 22 June 2021.

For the Commission
Stella KYRIAKIDES
Member of the Commission

COMMISSION IMPLEMENTING DECISION (EU) 2021/1037**of 16 June 2021****on the request for registration of the European citizens' initiative entitled 'Ban Fossil Fuel Advertising and Sponsorships' pursuant to Regulation (EU) 2019/788 of the European Parliament and of the Council****(Only the English text is authentic)**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2019/788 of the European Parliament and of the Council of 17 April 2019 on the European citizens' initiative ⁽¹⁾, and in particular Article 6(2) and (3) thereof,

Whereas:

- (1) A request for registration of the European citizens' initiative entitled 'Ban Fossil Fuel Advertising and Sponsorships' was submitted to the Commission on 22 April 2021.
- (2) The objectives of the initiative are expressed as follows: 'We call on the European Commission to propose an EU legislative act: prohibiting advertisements for fossil fuels, as well as air, road and water-borne transportation (other than transport services of general economic interest) powered by fossil fuels; prohibiting advertisements from any undertakings active in the market for fossil fuels, in particular by extracting, refining, supplying, distributing or selling fossil fuels; prohibiting sponsorships by undertakings defined under point 2 above, or using trademarks or commercial names used for fossil fuels. This law would fall into the EU competence, in that it would consist in an internal market regulation aimed at enhancing consumer protection, as well as a high level of public health and environmental protection. Indeed, this legislation would increase public awareness of products and technologies that are responsible for climate change and other environmental and health harms. As such, it would pursue objectives that are envisaged by the EU environmental and consumer protection policies, via the harmonisation of rules on fossil fuel advertisements and sponsorships. This would fall under shared competences including (see Article 4 TFEU), internal market, environment, consumer protection.'
- (3) An annex provides further details on the subject matter, objectives and background to the initiative. In particular, it clarifies that the fossil fuel products concerned include oil, fossil gas and coal. It further clarifies the scope of the proposed/requested ban, which, according to the organisers, should cover any promotion or advertising, direct or indirect, as well as any free or promotional distribution, or any sponsorship relationship; the ban should apply both offline and online, and cover advertising and sponsorship notably in the context of sport, education, science, public events and third party media events. Finally, the annex explains the reasons behind the initiative, as follows: (1) 'Fossil fuels are perpetuating the climate crisis, and should not be advertised', (2) 'Fossil fuels have created a public health crisis, and should not be advertised', (3) 'Fossil fuel companies are misleading consumers, and some have been found to be breaking advertising guidelines' and (4) 'Fossil fuel sponsorships are being used for political access'.
- (4) The group of organisers has also submitted a draft legal act entitled 'Ban Fossil Fuel Advertisements and Sponsorships: ECI Directive'. The scope of the draft legal act is 'the advertising of fossil fuel products, fossil fuel undertakings, and their promotion: (a) in the press and other printed publications; (b) in all forms of audiovisual commercial communications; (c) in radio broadcasting; (d) in information society services; and (e) through fossil fuel-related sponsorship, including the free or discounted distribution of fossil fuel products.'
- (5) Insofar as the initiative aims at preserving, protecting and improving the quality of the environment, protecting human health and prudent and rational utilisation of natural resources, the Commission has the power to present a proposal for a legal act on the basis of Article 192 of the Treaty.

⁽¹⁾ OJ L 130, 17.5.2019, p. 55.

- (6) Insofar as there are differences between national rules which are such as to create obstacles to trade and obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market or to cause significant distortions of competition, the Commission has the power to present a proposal for a legal act approximating the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market on the basis of Article 114 of the Treaty.
- (7) For these reasons, none of the parts of the initiative manifestly falls outside the framework of the Commission's powers to submit a proposal for a legal act of the Union for the purpose of implementing the Treaties.
- (8) This conclusion is without prejudice to the assessment of whether the concrete factual and substantive conditions required for the Commission to act, including proportionality and compatibility with fundamental rights, would be met in this case.
- (9) The group of organisers has provided appropriate evidence that it fulfils the requirements laid down in Article 5(1) and (2) of Regulation (EU) 2019/788 and has designated the contact persons in accordance with Article 5(3), first subparagraph, of that Regulation.
- (10) The initiative is not manifestly abusive, frivolous or vexatious, nor is it manifestly contrary to the values of the Union as set out in Article 2 of the Treaty on European Union and rights enshrined in the Charter of Fundamental Rights of the European Union.
- (11) The initiative entitled 'Ban Fossil Fuel Advertising and Sponsorships' should therefore be registered,

HAS ADOPTED THIS DECISION:

Article 1

The European citizens' initiative entitled 'Ban Fossil Fuel Advertising and Sponsorships' shall be registered.

Article 2

This Decision is addressed to the group of organisers of the European citizens' initiative entitled 'Ban Fossil Fuel Advertising and Sponsorships', represented by Ms Silvia PASTORELLI and Ms Sílvia DÍAZ PÉREZ acting as contact persons.

Done at Brussels, 16 June 2021.

For the Commission
Věra JOUROVÁ
Vice-President

COMMISSION DECISION (EU) 2021/1038**of 23 June 2021****granting a transitional period to the Kingdom of the Netherlands pursuant to Decision 2008/477/EC as regards an update of relevant technical conditions applicable to the 2 500-2 690 MHz frequency band***(notified under document C(2021) 4433)***(Only the Dutch text is authentic)**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision) ⁽¹⁾, and in particular Article 4(5) thereof,

Having regard to Commission Decision 2008/477/EC of 13 June 2008 on the harmonisation of the 2 500-2 690 MHz frequency band for terrestrial systems capable of providing electronic communications services in the Community ⁽²⁾, and in particular Article 2(2) thereof,

Having regard to the request made by the Netherlands on 6 January 2021,

Whereas:

- (1) Decision 2008/477/EC provides that Member States are to designate and make available, on a non-exclusive basis, the 2 500-2 690 MHz frequency band for terrestrial systems capable of providing electronic communications services, in accordance with the parameters set out in the Annex to that Decision.
- (2) Article 2(2) of Decision 2008/477/EC provides that Member States implementing time division (TDD) duplex or 'downlink-only' use outside the 2 570 – 2 620 MHz sub-band on the date when that decision takes effect may request a transitional period for the implementation of that Decision, pursuant to Article 4(5) of Decision No 676/2002/EC.
- (3) The Netherlands has informed the Commission that, while authorisations have been granted for the use of the major part of the 2 570 – 2 620 MHz sub-band in accordance with Implementing Decision (EU) 2020/636 ⁽³⁾, two limited sections of the band, namely the 2 565-2 570 MHz and 2 685-2 690 MHz lots, are still subject to two authorisations implementing time division duplex (TDD) instead of frequency division duplex (FDD) that were granted in 2010 pursuant to Decision 2008/477/EC and will expire in 2030.
- (4) By letter of 6 January 2021 to the Commission, The Netherlands requested a transitional period pursuant to Article 2(2) of Decision 2008/477/EC in order to maintain the validity of the two abovementioned authorisations implementing TDD until their expiry. Those authorisations were granted by decisions of the Agentschap Telecom van het Ministerie van Economische Zaken en Klimaat. One authorisation was granted under reference number AT-EZK/7635162 dossier number 6781570-G1 and is valid from 3 January 2013 until 2 January 2030 and the other authorisation was granted under reference number AT-EZK/7937970 dossier number 6697351 and is valid from 11 May 2010 until 11 May 2030.
- (5) In support of its request, the Netherlands has provided sufficient information and justification. By maintaining during the transitional period the two existing authorisations which are used for the provision of public mobile communications services, the Dutch authorities avoid interrupting the provision of mobile communications services by the holders of these two authorisations and avoid disrupting the present competition level playing field situation on the mobile communications market in The Netherlands. Moreover, the extensive usage restrictions attached to the use of the two corresponding spectrum lots required that these authorisations not be included in the

⁽¹⁾ OJ L 108, 24.4.2002, p. 1.

⁽²⁾ OJ L 163, 24.6.2008, p. 37.

⁽³⁾ Commission Implementing Decision (EU) 2020/636 of 8 May 2020 amending Decision 2008/477/EC as regards an update of relevant technical conditions applicable to the 2 500–2 690 MHz frequency band (OJ L 149, 12.5.2020, p. 3).

definition and determination of the generally applicable spectrum cap. As a consequence, the transitional period will ensure stability in the competitive situation of the mobile communications market and not unduly defer the implementation of Decision 2008/477/EC in the Netherlands.

- (6) Moreover, the emission power limits attached to the use of that spectrum under the relevant authorisations are in line with the international coordination agreements concluded with the neighbouring Member States in order to ensure that no interference is created into those Member States. Consequently, the transitional period will not defer the implementation of Decision 2008/477/EC in neighbouring Member States.
- (7) The transitional period would also not go beyond what is necessary so as not to prevent the establishment of a common framework and harmonised technical conditions for the use of the 2 500-2 690 MHz band; restrictions in 2 685-2 690 MHz are provided to protect radio astronomy services in the adjacent band and the use of the 2 565-2 570 MHz frequency is restricted to protect adjacent FDD usage.
- (8) Therefore, this transitional period would ensure that the EU policy objectives in the band 2 500-2 690 MHz are achieved at minimum cost for each Member State and operator.
- (9) For these reasons, the requested transitional period appears justified and proportionate and would not unduly defer implementation of Decision 2008/477/EC in the Netherlands or in the other Member States or create undue differences in the competitive or regulatory situation between Member States.
- (10) The members of the Radio Spectrum Committee were consulted and indicated at their meetings of 9 and 10 March 2021 that they did not object to that transitional period,

HAS ADOPTED THIS DECISION:

Article 1

A transitional period is hereby granted to the Netherlands under Decision 2008/477/EC subject to the conditions laid down in that Decision.

Article 2

The Netherlands is hereby authorised to implement, until 11 May 2030 at the latest, time division duplex (TDD) instead of frequency division duplex (FDD) in the 2 565-2 570 MHz and 2 685-2 690 MHz sub-bands.

Article 3

The Netherlands shall continue to ensure that the implementation of TDD pursuant to Article 2 does not unduly defer implementation of Decision 2008/477/EC, does not create undue differences in the competitive or regulatory situations between Member States and does not affect the terrestrial systems capable of providing electronic communications services already operating or to be deployed in the 2 500-2 690 MHz frequency band in accordance with the technical parameters harmonised by Decision 2008/477/EC within other Member States.

Article 4

This Decision is addressed to the Kingdom of the Netherlands.

Done at Brussels, 23 June 2021.

For the Commission
Thierry BRETON
Member of the Commission

III

(Other acts)

EUROPEAN ECONOMIC AREA

DECISION OF THE EEA JOINT COMMITTEE No 130/2021

of 15 March 2021

amending Protocol 10 to the EEA Agreement, on simplification of inspections and formalities in respect of carriage of goods [2021/1039]

THE EEA JOINT COMMITTEE,

Having regard to the Agreement on the European Economic Area, and in particular Article 98 thereof,

Whereas:

- (1) The relevant provisions of Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code ⁽¹⁾ and Commission Regulation (EEC) No 2454/93 of 2 July 1993 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code ⁽²⁾ have been replaced by the relevant provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code ⁽³⁾, Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code ⁽⁴⁾ and Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code ⁽⁵⁾.
- (2) The legislation of the European Union on customs security measures has been amended, in particular by Commission Implementing Decision (EU) 2019/2151 of 13 December 2019 establishing the work programme relating to the development and deployment of the electronic systems provided for in the Union Customs Code ⁽⁶⁾.
- (3) The provisions of Protocol 10 on simplification of inspections and formalities in respect of carriage of goods ('Protocol 10') to the Agreement on the European Economic Area (the 'EEA Agreement') should be aligned with the amendments to the legislation of the European Union, in order to guarantee an equivalent level of security.
- (4) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ⁽⁷⁾ was incorporated into the EEA Agreement by Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement ⁽⁸⁾.
- (5) This Decision should not apply to Iceland and Liechtenstein. However, subject to a new Decision, it could be opened to those countries.

⁽¹⁾ OJ L 302, 19.10.1992, p. 1.⁽²⁾ OJ L 253, 11.10.1993, p. 1.⁽³⁾ OJ L 269, 10.10.2013, p. 1.⁽⁴⁾ OJ L 343, 29.12.2015, p. 1.⁽⁵⁾ OJ L 343, 29.12.2015, p. 558.⁽⁶⁾ OJ L 325, 16.12.2019, p. 168.⁽⁷⁾ OJ L 119, 4.5.2016, p. 1.⁽⁸⁾ OJ L 183, 19.7.2018, p. 23.

(6) Protocol 10 to the EEA Agreement should therefore be amended accordingly,

HAS ADOPTED THIS DECISION:

Article 1

Protocol 10 to the EEA Agreement shall be amended as set out in the Annex to this Decision.

Article 2

1. This Decision shall enter into force on 15 March 2021, provided that all notifications under Article 103(1) of the EEA Agreement have been made (*). It shall apply from 15 March 2021.
2. Pending the notifications referred to in paragraph 1, the European Union and Norway shall apply this Decision provisionally as from 15 March 2021.

Article 3

This Decision shall be published in the EEA Section of, and in the EEA Supplement to, the *Official Journal of the European Union*.

Done at Brussels, 15 March 2021.

For the EEA Joint Committee
The President
Clara GANSLANDT

The Secretaries
To the EEA Joint Committee
Hege M. HOFF
Mikołaj KARŁOWSKI

(*) Constitutional requirements indicated.

ANNEX

1. Articles 9a to 9g of Chapter IIa (CUSTOMS SECURITY MEASURES) of Protocol 10 to the Agreement on the European Economic Area ('Agreement') are replaced by the following:

'CHAPTER IIa

CUSTOMS SECURITY MEASURES*Article 9a***Definitions**

For the purposes of this Chapter:

- (a) "risk" shall mean the likelihood and the impact of an event occurring in connection with the entry, exit, transit, transfer and end-use of goods moved between the customs territory of one of the Contracting Parties and third countries and the presence of goods that are not in free circulation, which pose a threat to the security and safety of the Contracting Parties, to public health, to the environment or to consumers;
- (b) "risk management" shall mean the systematic identification of risk and implementation of all measures necessary for limiting exposure to risk. This includes activities such as collecting data and information, analysing and assessing risk, prescribing and taking action and regular monitoring and review of the process and its outcomes, based on sources and strategies defined by the Contracting Parties or internationally.
- (c) "items of correspondence" shall mean letters, postcards, braille letters and printed matter that are not liable to import or export duty;
- (d) "express consignment" shall mean a consignment conveyed by or under the responsibility of an integrated service of expedited/time-definite collection, transport, customs clearance and delivery of parcels whilst tracking the location of, and maintaining control over such items throughout the supply of the service;
- (e) "goods in postal consignment" shall mean goods other than items of correspondence, contained in a postal parcel or package and conveyed under the responsibility of or by an operator established in and designated by a Contracting Party to provide the international services governed by the Universal Postal Convention adopted on 10 July 1984 under the aegis of the United Nations Organisation, and conveyed in accordance with the provisions of that Convention;
- (f) "customs declaration" shall mean the act whereby a person indicates, in the prescribed form and manner, a wish to place goods under a given customs procedure, with an indication, where appropriate, of any specific arrangements to be applied;
- (g) "temporary storage declaration" means the act whereby a person indicates, in the prescribed form and manner, that goods are in temporary storage.

*Article 9b***General provisions concerning security and safety**

1. The Contracting Parties undertake to set up and apply to the carriage of goods to and from third countries the customs security measures set out in this Chapter and thus to ensure an equivalent level of security and safety at their external borders.
2. The Contracting Parties shall refrain from applying the customs security measures set out in this Chapter to the carriage of goods between their customs territories.
3. The Contracting Parties shall consult prior to the conclusion of any agreement with a third country in the areas covered by this Chapter in order to ensure consistency with the Agreement, particularly if the proposed agreement includes provisions that derogate from the customs security measures set out in this Chapter.

*Article 9c***Declarations prior to the entry and exit of goods**

1. For the purposes of security and safety, goods brought into the customs territories of the Contracting Parties from third countries shall be covered by an entry summary declaration with the exception of goods carried on means of transport only passing through the territorial waters or the airspace of the customs territories without a stop within those territories.
2. For the purposes of security and safety, goods exiting the customs territories of the Contracting Parties that are destined for third countries shall be covered by an exit summary declaration with the exception of goods carried on means of transport only passing through the territorial waters or the airspace of the customs territories without a stop within those territories.
3. The entry or exit summary declaration shall be lodged before the goods are brought into or leave the customs territories of the Contracting Parties.
4. Where there is an obligation to lodge an entry or exit summary declaration for goods entering or exiting the customs territories of the Contracting Parties but such a declaration has not been lodged, one of the persons referred to in paragraphs 5 or 6 shall immediately lodge such a declaration or, if permitted by the customs authorities, shall instead lodge a customs declaration or temporary storage declaration that shall contain at least the particulars required for an entry or exit summary declaration. In such circumstances, customs authorities shall carry out the risk analysis for security and safety purposes on those goods on the basis of the customs declaration or the temporary storage declaration.
5. Each Contracting Party shall determine the persons responsible for lodging exit summary declarations as well as specify the authorities competent to receive them.
6. The entry summary declaration shall be lodged by the carrier.

Notwithstanding the obligations of the carrier, the entry summary declaration may be lodged instead by one of the following persons:

- (a) the importer or consignee or other person in whose name or on whose behalf the carrier acts;
- (b) any person who is able to present the goods in question or have them presented at the customs office of first entry.

In specific cases, where all the particulars of the entry summary declaration necessary for risk analysis for security and safety purposes cannot be obtained from the persons referred to in the first sub-paragraph, other persons holding those particulars and the appropriate rights to provide them may be required to provide those particulars.

Each person submitting the particulars of the entry summary declaration shall be responsible for the particulars that he/she has submitted.

7. By derogation from paragraph 6 of this Article, until the dates of the deployment of the electronic system referred to in Article 1(1) of Annex I, each Contracting Party shall determine the persons who are required to lodge the entry summary declaration, the means for lodging it, for exchanging information relating to it and for requesting its amendment and/or invalidation.
8. The customs authorities of the Contracting Parties may define the cases in which a customs declaration or temporary storage declaration can be used as an entry or an exit summary declaration, provided that:
 - (a) the customs declaration or temporary storage declaration contains all the particulars required for an entry or exit summary declaration, and
 - (b) the replacing declaration is lodged prior to the expiry of the time limit at the competent customs office for lodging the entry or exit summary declaration.

9. Annex I lays down:

- the electronic system relating to the entry summary declaration,
- the form and the particulars of the entry or exit summary declaration,
- the exceptions from the obligation to lodge an entry or exit summary declaration,
- the place where the entry or exit summary declaration shall be lodged,
- the time limits for lodging the entry or exit summary declaration,
- the technical arrangements for the electronic systems used to lodge the entry summary declaration,
- the financing arrangement concerning the responsibilities, commitments and expectations upon the implementation and operation of the Import Control System 2,
- any other provision necessary to ensure the application of this Article.

Article 9d

Authorised economic operator

1. A Contracting Party shall grant, subject to the criteria laid down in Annex II, the status of 'authorised economic operator' for security purposes to any economic operator established in its customs territory.

Authorised economic operators shall enjoy facilitations in respect of security-related customs controls.

Subject to the rules and conditions set out in paragraph 2, the status of authorised economic operator granted by a Contracting Party shall be recognised by the other Contracting Party, without prejudice to customs inspections, particularly with a view to implementing agreements with third countries providing for arrangements for the mutual recognition of the status of authorised economic operator.

2. Annex II lays down:

- the rules for granting the status of authorised economic operator, and in particular the criteria for granting that status and the conditions for applying them,
- the type of facilitations that shall be accorded,
- the rules on the suspension, annulment and revocation of the status of authorised economic operator,
- the arrangements for exchanges of information between the Contracting Parties on their authorised economic operators,
- any other measure necessary for the application of this Article.

Article 9e

Security and safety related customs controls and security and safety related risk management

1. Security and safety related customs controls other than random checks, shall be primarily based on risk analysis using electronic data processing techniques with the purpose of identifying and evaluating the risks and developing the necessary counter-measures, on the basis of criteria developed by the Contracting Parties.

2. Security and safety related customs controls shall be performed within a common risk management framework, based upon the exchange of risk-related information and risk analysis results between the customs authorities of the Contracting Parties. The customs authority of Norway through its participation in the Customs Code Committee referred to in Article 9h(4) of Chapter IIa, shall contribute to establishing common risk criteria and standards, control measures and priority control areas in relation to the particulars of the entry and exit summary declarations. Controls based upon such information and criteria shall be carried out without prejudice to other customs controls.

3. The Contracting Parties shall use a Common Risk Management System for exchanging risk-related information, information on the implementation of common risk criteria and standards, of common priority control areas and of customs crisis management, and on risk analysis results and control results.
4. The Contracting Parties shall recognise the equivalence of their risk management systems related to security and safety.
5. The EEA Joint Committee shall adopt any other measure necessary for the application of this Article.

Article 9f

Monitoring the implementation of customs security measures

1. The EEA Joint Committee shall determine how the Contracting Parties are to monitor the implementation of this Chapter and to verify compliance with its provisions and those of the Annexes to this Protocol.
2. The monitoring referred to in paragraph 1 may take the form of:
 - regular assessments of the implementation of this Chapter, and in particular of the equivalence of customs security measures,
 - a review to improve the way in which it is applied or to amend its provisions so that it better fulfils its objectives,
 - the organisation of thematic meetings between experts of both Contracting Parties and audits of administrative procedures, including on-the-spot visits.
3. The EEA Joint Committee shall ensure that measures taken under this Article uphold the rights of economic operators.

Article 9g

Protection of professional secrecy and personal data

The information exchanged by the Contracting Parties as part of the measures provided for in this Chapter shall enjoy the protection extended to professional secrecy and personal data as defined in the relevant laws applicable in the territory of the recipient Contracting Party.

In particular, that information may not be further transferred to persons other than the competent authorities in the recipient Contracting Party, nor may it be used by those authorities for purposes other than those provided for in the Agreement.'

2. Annexes I and II of Protocol 10 to the Agreement are replaced by the following:

'ANNEX I

ENTRY AND EXIT SUMMARY DECLARATIONS

TITLE I

Entry summary Declaration*Article 1***Electronic System relating to the entry summary declaration**

1. The electronic Import Control System 2 (ICS2) shall be used for:
 - (a) submitting, processing and storing the particulars of the entry summary declarations and other information relating to those declarations, relating to risk analysis for customs security and safety purposes, including the support of aviation security, and relating to the measures that must be taken based on the results of that analysis;
 - (b) exchanging information concerning the particulars of the entry summary declaration and results of risk analysis of entry summary declarations, concerning other information necessary to perform that risk analysis, and concerning measures undertaken on the basis of risk analysis, including recommendations on places of control and the results of those controls;
 - (c) exchanging information for monitoring and evaluating the implementation of the common security and safety risk criteria and standards and of the control measures and priority control areas.
2. The development and release dates of the sequenced deployment of the electronic system referred to in this Annex are the dates set out in the Union Customs Code project Import Control System 2 (ICS2) set out in the Annex to Commission Implementing Decision (EU) 2019/2151 ⁽¹⁾.

The Contracting Parties are expected to be ready at the same time for each release at the start of the deployment window. Where deemed appropriate, the Contracting Parties may allow the economic operators to gradually connect to the system until the end of the deployment window provided for each of the releases. The Contracting Parties shall publish the deadlines and instructions for economic operators on their website.

3. Economic operators shall use a harmonised trader interface, designed by the Contracting Parties in agreement with each other, for submissions, requests for amendments, requests for invalidations, processing and storage of the particulars of entry summary declarations and for the exchange of related information with the customs authorities.
4. The customs authorities of the Contracting Parties may permit commercial, port or transport information systems to be used for lodging the particulars of the entry summary declaration, provided such systems contain the necessary particulars and those particulars are available within the time limits referred to in Article 7.

*Article 2***Form and content of the entry summary declaration**

1. The entry summary declaration, and the notification of arrival of a seagoing vessel or of an aircraft shall contain the particulars laid down in the following columns of Annex B to Commission Delegated Regulation (EU) 2015/2446 ⁽²⁾:
 - (a) F10 to F16;

⁽¹⁾ Deployment window of release 1 of ICS2: from 15.3.2021 to 1.10.2021; deployment window of release 2 of ICS2: from 1.3.2023 to 2.10.2023; deployment window of release 3 of ICS2: from 1.3.2024 to 1.10.2024;
Commission Implementing Decision (EU) 2019/2151 of 13 December 2019 establishing the work programme relating to the development and deployment of the electronic systems provided for in the Union Customs Code (OJ L 325, 16.12.2019, p. 168).

⁽²⁾ Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code (OJ L 343 29.12.2015, p. 1), last amended by Commission Delegated Regulation (EU) 2021/234 of 7 December 2020 (OJ L 63, 23.2.2021, p. 1).

- (b) F20 to F33;
- (c) F40 to F45;
- (d) F50 and F51;
- (e) G2.

The particulars of the entry summary declaration shall comply with the respective formats, codes and cardinalities set out in Annex B to Commission Implementing Regulation (EU) 2015/2447 ⁽³⁾ and be completed in accordance with the notes in those Annexes.

2. The particulars of the entry summary declaration may be provided by the submission of more than one dataset by more than one person.
3. The electronic system referred to in Article 1(1) shall be used for lodging a request for amendment or invalidation of an entry summary declaration or the particulars therein.

Where more than one person requests an amendment or an invalidation of the particulars of the entry summary declaration, each of those persons shall only be permitted to request the amendment or the invalidation of the particulars that he/she submitted.

4. The customs authorities of the Contracting Party, who registered the entry summary declaration, shall immediately notify the person who lodged the request for amendment or invalidation of their decision to register it or reject it.

Where the amendments to or invalidation of the particulars of the entry summary declaration are lodged by a person different from the carrier, the customs authorities shall also notify the carrier, provided that the carrier has requested to be notified and has access to the electronic system referred to in Article 1(1).

5. In accordance with Article 9c(8) of this Protocol, until the date of the deployment of release 3 of the system referred to in Article 1(1) of this Annex, the Contracting Parties may carry out the security and safety related risk analysis on the basis of the transit declaration lodged in the New Computerised Transit System (NCTS) in accordance with the Convention on a Common Transit Procedure ⁽⁴⁾, including the exchange of risk analysis related information between the involved Contracting Parties, for goods transported by sea, inland waterways, road and rail. NCTS is the electronic system that enables communication between the Contracting Parties, and between the Contracting Parties and economic operators for the purposes of submitting customs declaration for transit including all the particulars required for an entry or exit summary declaration and the notifications relating to those goods.

Before the deployment of release 3 of the system referred to in Article 1(1) of this Annex, the Contracting Parties shall assess whether or not, after that date, the customs authorities may continue to carry out the risk analysis on the basis of the transit declaration containing the particulars of an entry summary declaration lodged in NCTS ⁽⁵⁾ and shall modify the Agreement if necessary.

Article 3

Waiver from the obligation to lodge an entry summary declaration

1. An entry summary declaration shall not be required in respect of the following goods:

- (a) electrical energy;

⁽³⁾ Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code (OJ L 343 29.12.2015, p. 558), last amended by Commission Implementing Regulation (EU) 2021/235 of 8 February 2021 (OJ L 63, 23.2.2021, p. 386).

⁽⁴⁾ Convention between the European Economic Community, the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation on a common transit procedure of 20 May 1987 (OJ L 226, 13.8.1987, p. 2, including previous and future amendments as agreed upon by the Joint Committee of the aforementioned Convention).

⁽⁵⁾ The NCTS is upgraded to cover the new security requirements from Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (OJ L 269, 10.10.2013, p. 1), last amended by Regulation (EU) 2019/632 of the European Parliament and of the Council of (OJ L 111, 25.4.2019, p. 54). The deployment of the phased update of the NCTS is set out in the Annex to the Commission Implementing Decision (EU) 2019/2151.

- (b) goods entering by pipeline;
- (c) items of correspondence;
- (d) goods in postal consignments, as follows:
 - (1) where the postal consignments are transported by air and have a Contracting Party as final destination, until the date set out for the deployment of release 1 of the electronic system referred to in Article 1(1);
 - (2) where the postal consignments are transported by air and have a third country or third territory as final destination, until the date set out for the deployment of release 2 of the electronic system referred to in Article 1(1);
 - (3) where the postal consignments are transported by sea, inland waters, road or rail, until the date set out for the deployment of release 3 of the electronic system referred to in Article 1(1);
- (e) goods for which an oral customs declaration or simple crossing of the border is permitted under the rules laid down by the Contracting Parties, provided that they are not carried under a transport contract;
- (f) goods contained in travellers' personal baggage;
- (g) goods covered by ATA or CPD Carnets provided they are not carried under a transport contract;
- (h) goods entitled to relief pursuant to the Vienna Convention of 18 April 1961 on Diplomatic Relations, the Vienna Convention of 24 April 1963 on Consular Relations or other consular conventions or the New York Convention of 16 December 1969 on Special Missions;
- (i) weapons and military equipment brought into the customs territory of one of the Contracting Parties by the authorities in charge of the military defence of the territory, in military transport or transport operated for the sole use of the military authorities;
- (j) the following goods brought into the customs territory of one of the Contracting Parties directly from offshore installations operated by a person established in the customs territory of one of the Contracting Parties:
 - (1) goods which were incorporated in those offshore installations for the purposes of their construction, repair, maintenance or conversion;
 - (2) goods which were used to fit or equip the said offshore installations;
 - (3) provisions used or consumed on the said offshore installations;
 - (4) non-hazardous waste from the said offshore installations;
- (k) goods in consignments the intrinsic value of which does not exceed EUR 22, provided that the customs authorities accept, with the agreement of the economic operator, to carry out risk analysis using the information contained in, or provided by, the system used by the economic operator, as follows:
 - (1) where the goods are in express consignments, that are transported by air, until the date set out for the deployment of release 1 of the electronic system referred to in Article 1(1);
 - (2) where the goods are transported by air other than in postal or express consignments, until the date set out for the deployment of release 2 of the electronic system referred to in Article 1(1);
 - (3) where the goods are transported by sea, inland waterways, road or rail, until the date set out for the deployment of release 3 of the electronic system referred to in Article 1(1);
- (l) goods moved under cover of the NATO form 302 provided for in the Convention between the Parties to the North Atlantic Treaty regarding the Status of their Forces, signed in London on 19 June 1951, or under cover of the EU form 302 provided for in point 51 of Article 1 of Commission Delegated Regulation (EU) 2015/2446;
- (m) goods brought to one of the Contracting Parties from Ceuta and Melilla, Heligoland, the Republic of San Marino, the Vatican City State, the municipality of Livigno and the Swiss customs exclaves of Samnaun and Sempuoir;

- (n) the following goods on board vessels and aircraft:
 - (1) goods which have been supplied for incorporation as parts of or accessories in those vessels and aircraft;
 - (2) goods for the operation of the engines, machines and other equipment of those vessels or aircraft;
 - (3) foodstuffs and other items to be consumed or sold on board;
- (o) products of sea-fishing and other products taken from the sea outside the customs territories of the Contracting Parties by their fishing vessels;
- (p) vessels, and the goods carried thereon, entering the territorial waters of one of the Contracting Parties with the sole purpose of taking on board supplies without connecting to any of the port facilities;
- (q) household effects as defined in the legislation of the respective Contracting Parties provided that they are not carried under a transport contract.

2. An entry summary declaration shall not be required in the cases provided for in an international agreement concluded between a Contracting Party and a third country on security, subject to the procedure laid down in Article 9b(3) of this Protocol.

3. An entry summary declaration shall not be required in cases where the goods temporarily leave the customs territories of the Contracting Parties during transport by sea or air between two points of those customs territories and without having stopped in a third country.

Article 4

Place for lodging an entry summary declaration

1. The entry summary declaration shall be lodged at the customs office that is competent for customs supervision at the place in the customs territory of one of the Contracting Parties where the means of transport carrying the goods arrives or, where applicable, is destined to arrive, from a third country or a third territory (hereafter referred to as the “customs office of first entry”).
2. Where the entry summary declaration is lodged by the submission of more than one dataset, or by the submission of the minimum dataset, the person submitting the partial or minimum dataset shall do so to the customs office that, according to his/her knowledge, should be the customs office of first entry. If that person does not know the place in the customs territories of the Contracting Parties at which the means of transport carrying the goods is expected to first arrive, the customs office of first entry may be determined based on the place to which the goods are consigned.
3. The customs authorities of the Contracting Parties may allow the entry summary declaration to be lodged at another customs office, provided that the latter immediately communicates or makes available electronically the necessary particulars to the customs office of first entry.

Article 5

Registration of an entry summary declaration

1. The customs authorities shall register each submission of particulars of the entry summary declaration upon its receipt and shall immediately notify the declarant or its representative of its registration and shall communicate a Master Reference Number of the submission and the date of registration to that person.
2. From the date of the deployment of release 2 of the electronic system referred to in Article 1(1), where the entry summary declaration is lodged by a person other than the carrier, the customs authorities shall immediately notify the carrier of the registration, provided that the carrier has requested to be notified and has access to that electronic system.

*Article 6***Lodging of an entry summary declaration**

Where none of the waivers from the obligation to lodge an entry summary declaration in Article 9c of this Protocol and Article 3 of this Annex applies, the particulars of the entry summary declaration shall be provided as follows:

- (a) for goods transported by air,
 - (1) express carriers shall lodge, for all consignments, the minimum dataset from the date of the deployment of release 1 of the electronic system referred to in Article 1(1) of this Annex;
 - (2) postal operators shall lodge, for all consignments having a Contracting Party as final destination, the minimum dataset from the date of the deployment of release 1 of the electronic system referred to in Article 1(1) of this Annex;
 - (3) by the submission of one or more than one dataset through the electronic system referred to in Article 1(1) of this Annex, from the date of the deployment of release 2 of that system;
- (b) for goods transported by sea, inland waterways, road and rail, by the submission of one or more than one dataset through the electronic system referred to in Article 1(1) of this Annex, from the date of the deployment of release 3 of that system.

*Article 7***Time limits for lodging an entry summary declaration**

1. Where the goods are brought into the customs territories of the Contracting Parties by sea, the entry summary declaration shall be lodged within the following time limits:

- (a) for containerised cargo, other than where point (c) or point (d) applies, at the latest 24 hours before the goods are loaded onto the vessel on which they are to be brought into the customs territories of the Contracting Parties;
- (b) for bulk or break bulk cargo, other than where point (c) or (d) applies, at the latest four hours before the arrival of the vessel at the first port of entry into the customs territories of the Contracting Parties;
- (c) at the latest two hours before arrival of the vessel at the first port of entry into the customs territories of the Contracting Parties in the case of goods coming from any of the following:
 - (1) Greenland;
 - (2) the Faeroe Islands;
 - (3) Iceland;
 - (4) ports on the Baltic Sea, the North Sea, the Black Sea and the Mediterranean Sea;
 - (5) all ports of Morocco;
 - (6) ports of the United Kingdom of Great Britain and Northern Ireland, with the exception of ports located in Northern Ireland, and ports of the Channel Islands and the Isle of Man;
- (d) for movement, other than where point (c) applies, between a territory outside the customs territories of the Contracting Parties and the French overseas departments, the Azores, Madeira or the Canary Islands, where the duration of the voyage is less than 24 hours, at the latest two hours before arrival at the first port of entry into the customs territories of the Contracting Parties.

2. Where the goods are brought into the customs territories of the Contracting Parties by air, the full particulars of the entry summary declaration shall be lodged as soon as possible and in any case within the following time limits:

- (a) for flights with a duration of less than four hours, at the latest by the time of the actual departure of the aircraft;
- (b) for other flights, at the latest four hours before the arrival of the aircraft at the first airport in the customs territories of the Contracting Parties.

3. From the date of the deployment of release 1 of the electronic system referred to in Article 1(1), postal operators and express carriers shall lodge at least the minimum dataset of the entry summary declaration as soon as possible and at the latest before the goods are loaded onto the aircraft on which they are to be brought into the customs territories of the Contracting Parties.

4. From the date of the deployment of release 2 of the electronic system referred to in Article 1(1), economic operators other than postal operators and express carriers shall lodge at least the minimum dataset of the entry summary declaration as soon as possible and at the latest before the goods are loaded onto the aircraft on which they are to be brought into the customs territories of the Contracting Parties.

5. From the date of the deployment of release 2 of the electronic system referred to in Article 1(1), where only the minimum dataset of the entry summary declaration has been provided within the time limits referred to in paragraphs 3 and 4 of this Article, the other particulars shall be provided within the time limits specified in paragraph 2 of this Article.

6. Until the date of the deployment of release 2 of the electronic system referred to in Article 1(1), the minimum dataset of the entry summary declaration lodged in accordance with paragraph 3 of this Article shall be considered as the full entry summary declaration for goods in postal consignments having a Contracting Party as final destination and for goods in express consignments with an intrinsic value not exceeding EUR 22.

7. Where the goods are brought into the customs territories of the Contracting Parties by rail, the entry summary declaration shall be lodged within the following time limits:

- (a) where the train voyage from the last train formation station located in a third country to the customs office of first entry takes less than two hours, at the latest one hour before arrival of the goods at the place for which that customs office is competent;
- (b) in all other cases, at the latest two hours before the arrival of the goods at the place for which the customs office of first entry is competent.

8. Where the goods are brought into the customs territories of the Contracting Parties by road, the entry summary declaration shall be lodged at the latest one hour before the arrival of the goods at the place for which the customs office of first entry is competent.

9. Where the goods are brought into the customs territories of the Contracting Parties by inland waterways, the entry summary declaration shall be lodged at the latest two hours before arrival of the goods at the place for which the customs office of first entry is competent.

10. Where the goods are brought into the customs territories of the Contracting Parties on a means of transport which is, itself, transported on an active means of transport, the time limit for lodging the entry summary declaration shall be the time limit applicable to the active means of transport.

11. The time limits referred to in paragraphs 1 to 10 shall not apply in the case of *force majeure*.

12. Subject to the procedure referred to in Article 9b(3) of this Protocol, the time limits mentioned in paragraphs 1 to 10 of this Article shall not apply where international agreements on security between a Contracting Party and third countries provide otherwise.

Article 8

Security and safety related risk analysis and security and safety related customs controls relating to the entry summary declarations

1. Risk analysis shall be completed before the arrival of the goods at the customs office of first entry, provided that the entry summary declaration has been lodged within the time limits laid down in Article 7, unless a risk is identified or an additional risk analysis needs to be carried out.

Without prejudice to the first subparagraph of this paragraph, a first risk analysis on goods to be brought into the customs territories of the Contracting Parties by air shall be carried out as soon as possible upon receipt of the minimum dataset of the entry summary declaration referred to in Article 7(3) and (4).

2. The customs office of first entry shall complete the risk analysis for security and safety purposes after the following exchange of information through the electronic system referred to in Article 1(1):

- (a) immediately after registration, the customs office of first entry shall make the particulars of the entry summary declaration available to the customs authorities of the Contracting Parties indicated in those particulars and to the customs authorities of the Contracting Parties that have recorded in the electronic system information relating to security and safety risks that matches particulars of that entry summary declaration;
- (b) within the time limits laid down in Article 7, the customs authorities of the Contracting Parties referred to in point (a) of this paragraph shall perform a risk analysis for security and safety purposes and, if they identify a risk, they shall make the results available to the customs office of first entry;
- (c) the customs office of first entry shall take into account the information on risk analysis results provided by the customs authorities of the Contracting Parties referred in point (a) to complete the risk analysis;
- (d) the customs office of first entry shall make the results of the completed risk analysis available to the customs authorities of the Contracting Parties that contributed to the risk analysis and to those that are potentially concerned by the movement of the goods;
- (e) the customs office of first entry shall notify the completion of the risk analysis to the following persons, provided that they have requested to be notified and have access to the electronic system referred to in Article 1(1):
 - the declarant or his/her representative;
 - the carrier, if different from the declarant and his/her representative.

3. Where the customs office of first entry requires further information on the particulars of the entry summary declaration for the completion of the risk analysis, that analysis shall be completed after that information has been provided.

For those purposes, the customs office of first entry shall request that information from the person that lodged the entry summary declaration or, where applicable, the person that submitted the particulars of the entry summary declaration. Where that person is different from the carrier, the customs office of first entry shall inform the carrier, provided that the carrier has requested to be notified and has access to the electronic system referred to in Article 1(1).

4. Where the customs office of first entry has reasonable grounds to suspect that goods brought by air could pose a serious aviation security threat, it shall require that the consignment, before being loaded on an aircraft bound for the customs territories of the Contracting Parties, be screened as High Risk Cargo and Mail in accordance with Annex XIII Part I point VI, Articles 66h and 66hf, of the Agreement laying down detailed measures for the implementation of the common basic standards on aviation security.

The customs office of first entry shall notify the following persons, provided that they have access to the electronic system referred to in Article 1(1):

- (a) the declarant or his/her representative;
- (b) the carrier, if different from the declarant and his/her representative.

Following that notification, the person who lodged the entry summary declaration, or where applicable, the person that submitted the particulars of the entry summary declaration shall provide the customs office of first entry with the results of that screening and with all other related relevant information. The risk analysis shall only be completed after that information has been provided.

5. Where the customs office of first entry has reasonable grounds to consider that goods brought by air or containerised cargo brought by sea, as referred to in Article 7(1)(a), would pose such a serious threat to security and safety that immediate action is required, it shall direct that the goods are not to be loaded on the relevant means of transport.

The customs office of first entry shall notify the following persons, provided that they have access to the electronic system referred to in Article 1(1):

- (a) the declarant or his/her representative;
- (b) the carrier, if different from the declarant and his/her representative.

That notification shall be made immediately after the detection of the relevant risk and, in the case of containerised cargo brought by sea as referred to in Article 7(1)(a), at the latest within 24 hours of the receipt of the entry summary declaration or, where applicable, of the particulars of the entry summary declaration by the carrier.

The customs office of first entry shall also immediately inform the customs authorities of the Contracting Parties of that notification and make the relevant particulars of the entry summary declaration available to them.

6. Where a consignment has been identified as posing a threat of such nature that immediate action is required upon arrival of the means of transport, the customs office of first entry shall take that action upon arrival of the goods.

7. After completing the risk analysis, the customs office of first entry may recommend, through the electronic system referred to in Article 1(1), the most appropriate place and measures to carry out a control.

The customs office competent for the place that has been recommended as the most appropriate for control shall decide on the control and shall make, through the electronic system referred to in Article 1(1), the results of that decision available to all the customs offices of the Contracting Parties potentially concerned by the movement of goods, at the latest at the moment of presentation of the goods at the customs office of first entry.

8. The customs offices shall make the results of their security and safety related customs controls available to other customs authorities of the Contracting Parties through the system referred to in Article 1(1) where:

- (a) the risks are assessed by a customs authority as being significant and requiring customs control and the results of the control establish that the event triggering the risks has occurred; or
- (b) the control results do not establish that the event triggering the risks has occurred, but the customs authority concerned considers the threat to present a high risk elsewhere in the customs territories of the Contracting Parties; or
- (c) it is necessary for a uniform application of the rules in the Agreement.

The Contracting Parties shall exchange in the system referred to in Article 9e(3) of this Protocol the information on the risks mentioned under points a) and b).

9. Where goods for which the obligation to lodge an entry summary declaration is waived in accordance with Article 3(1) (c) to (f), (h) to (m), (o) and (q) are brought into the customs territories of the Contracting Parties, the risk analysis shall be carried out upon the presentation of the goods.

10. Goods presented to customs may be released as soon as the risk analysis has been carried out and the results of the risk analysis and, where required, the measures taken, allow such a release.

11. Risk analysis shall also be carried out if the particulars of the entry summary declaration are amended in accordance with Article 2(3) and (4). In that case, without prejudice to the time limit laid down in the third subparagraph of paragraph 5 of this Article for containerised cargo brought by sea, the risk analysis shall be completed immediately upon receipt of those particulars unless a risk is identified or an additional risk analysis needs to be carried out.

*Article 9***Provision of particulars of an entry summary declaration by other persons**

1. From the date set out for the deployment of release 2 of the electronic system referred to in Article 1(1), where for the same goods transported by air, one or more persons other than the carrier have concluded one or more transport contracts covered by one or more air waybills, the following rules apply:

- (a) the person issuing an air waybill shall inform the person who concluded a transport contract with him/her of the issuance of that air waybill;
- (b) in the case of a goods co-loading arrangement, the person issuing the air waybill shall inform the person with whom he/she entered into that arrangement of the issuance of that air waybill;
- (c) the carrier and any of the persons issuing an air waybill shall provide, in the particulars of the entry summary declaration, the identity of any person that did not make the particulars required for the entry summary declaration available to them;
- (d) if the person issuing the air waybill does not make the particulars required for the entry summary declaration available to his/her contractual partner who issues an air waybill to him/her, or to his/her contractual partner with whom he/she concluded a goods co-loading arrangement, the person who does not make the required particulars available shall provide those particulars to the customs office of first entry.

2. From the date set out for the deployment of release 2 of the electronic system referred to in Article 1(1), where the postal operator does not make the particulars required for the entry summary declaration of postal consignments available to the carrier that is obliged to lodge the rest of the particulars of the declaration through that system, the following rules apply:

- (a) the postal operator of destination, if the goods are consigned to the Contracting Parties, or the postal operator of the Contracting Parties of first entry, if the goods are transiting through the Contracting Parties, shall provide those particulars to the customs office of first entry; and
- (b) the carrier shall provide, in the particulars of the entry summary declaration, the identity of the postal operator that does not make the particulars required for the entry summary declaration available to him/her.

3. From the date set out for the deployment of release 2 of the electronic system referred to in Article 1(1), where the express carrier does not make the particulars required for the entry summary declaration of express consignments transported by air available to the carrier, the following rules apply:

- (a) the express carrier shall provide those particulars to the customs office of first entry; and
- (b) the carrier shall provide, in the particulars of the entry summary declaration, the identity of the express carrier that does not make the particulars required for the entry summary declaration available to him/her.

4. From the date set out for the deployment of release 3 of the electronic system referred to in Article 1(1), where, in the case of transport by sea or inland waterways, for the same goods, one or more additional transport contracts covered by one or more bills of lading have been concluded by one or more persons other than the carrier, the following rules apply:

- (a) the person issuing the bill of lading shall inform the person that concluded a transport contract with him/her about the issuance of that bill of lading;
- (b) in the case of a goods co-loading arrangement, the person issuing the bill of lading shall inform the person with whom he/she entered into that arrangement of the issuance of that bill of lading;
- (c) the carrier and any of the persons issuing a bill of lading shall provide, in the particulars of the entry summary declaration, the identity of any person that has concluded a transport contract with them and has not provided them with the particulars required for the entry summary declaration;

- (d) the person issuing the bill of lading shall provide, in the particulars of the entry summary declaration, the identity of the consignee indicated in the bill of lading as not having underlying bills of lading that has not made the particulars required for the entry summary declaration available to him/her;
- (e) if the person issuing the bill of lading does not make the particulars required for the entry summary declaration available to his/her contractual partner who issues a bill of lading to him/her, or to his/her contractual partner with whom he/she concluded a goods co-loading arrangement, the person who does not make the required particulars available shall provide those particulars to the customs office of first entry;
- (f) if the consignee indicated in the bill of lading that has no underlying bills of lading does not make the particulars required for the entry summary declaration available to the person issuing that bill of lading, he/she shall provide those particulars to the customs office of first entry.

Article 10

Diversion of a sea-going vessel or an aircraft entering the customs territory of the Contracting Parties

1. From the date set out for the deployment window of release 2 of the electronic system referred to in Article 1(1), where an aircraft is diverted and has arrived in the first place at a customs office located in a country that was not indicated as a country of routing in the entry summary declaration, the actual customs office of first entry shall, through that system, retrieve the particulars of the entry summary declaration, the risk-analysis results and the control recommendations made by the expected customs office of first entry.
2. From the date set out for the deployment window of release 3 of the electronic system referred to in Article 1(1), where a sea-going vessel is diverted and has arrived in the first place at a customs office located in a country that was not indicated as a country of routing in the entry summary declaration, the actual customs office of first entry shall, through that system, retrieve the particulars of the entry summary declaration, the risk-analysis results and the control recommendations made by the expected customs office of first entry.

TITLE II

technical arrangements for the Import Control System 2

Article 11

Import Control System 2

1. The ICS2 shall support communication between the economic operators and the Contracting Parties for the purposes of fulfilment of entry summary declaration requirements, risk analysis by the Contracting Parties' customs authorities for security and safety purposes and customs measures aimed to mitigate such risks including security and safety related customs controls, and the communication between the Contracting Parties for the purpose of fulfilment of entry summary declaration requirements.
2. The ICS2 shall consist of the following common components developed at Union level:
 - (a) a shared trader interface;
 - (b) a common repository.
3. Norway shall develop a national entry system as a national component available in Norway.
4. Norway may develop a national trader interface as a national component available in Norway.
5. The ICS2 shall be used for the following purposes:
 - (a) submitting, processing and storing the particulars of the entry summary declarations, requests for amendments and invalidations in accordance with Article 9c of this Protocol and this Annex;

- (b) receiving, processing and storing the particulars of entry summary declarations extracted from the declarations referred to in Article 9c of this Protocol and this Annex;
- (c) submitting, processing and storing of information regarding arrival and notifications of arrival of a sea-going vessel or an aircraft in accordance with Article 9c of this Protocol and this Annex;
- (d) receiving, processing and storing of information regarding presentation of goods to customs authorities of the Contracting Parties in accordance with Article 9c of this Protocol and this Annex;
- (e) receiving, processing and storing of information regarding risk analysis requests and results, control recommendations, decisions on controls, and control results in accordance with Articles 9c and 9e of this Protocol and this Annex;
- (f) receiving, processing, storing and communicating of the notifications and information to and from the economic operators in accordance with Articles 9c and 9e of this Protocol and this Annex;
- (g) submitting, processing and storing of information by the economic operators requested by customs authorities of the Contracting Parties in accordance with Articles 9c and 9e of this Protocol and this Annex.

6. The ICS2 shall be used to support the monitoring and evaluating by the Contracting Parties of the implementation of the common security and safety risk criteria and standards and of the control measures and priority control areas referred to in Article 9e of this Protocol.

7. The authentication and access verification of economic operators for the purposes of access to the common components of the ICS2 shall be effected using the Uniform User Management and Digital Signature (hereinafter referred to as "UUM&DS") platform referred to in Article 13.

8. The authentication and access verification of Contracting Parties' officials for the purposes of access to the common components of the ICS2 shall be effected using the network services provided by the Union.

9. The harmonised trader interface shall be an entry point to the ICS2 for economic operators in accordance with Article 1.

10. The harmonised trader interface shall interoperate with the ICS2 common repository referred to in paragraphs 12 to 14.

11. The harmonised trader interface shall be used for submissions, requests for amendments, request for invalidations, processing and storage of the particulars of the entry summary declarations and notifications of arrival, as well as exchange of information between the Contracting Parties and economic operators.

12. The ICS2 common repository shall be used by the Contracting Parties for processing of the particulars of entry summary declarations, requests for amendment, requests for invalidation, notifications of arrival, information regarding presentation of goods, information regarding risk analysis requests and results, control recommendations, control decisions, and control results and information exchanged with economic operators.

13. The ICS2 common repository shall be used by the Contracting Parties for the purpose of statistics and evaluation, and for the exchange of entry summary declaration information between the Contracting Parties.

14. The ICS2 common repository shall interoperate with the harmonised trader interface, national trader interfaces where developed by the Contracting Parties, and with the national entry systems.

15. The customs authority of a Contracting Party shall use the common repository to consult a customs authority of the other Contracting Party in accordance with Articles 9c and 9e of this Protocol and this Annex before completing the risk analysis for security and safety purposes. The customs authority of a Contracting Party shall also use the common repository to consult with the other Contracting Party on the recommended controls, decisions taken with regard to recommended controls and on the results of security and safety related customs controls in accordance with Articles 9c and 9e of this Protocol and this Annex.

16. The national trader interface, where developed by the Contracting Parties, shall be an entry point to the ICS2 for economic operators in accordance with Article 1 where the submission is addressed to the Contracting Party operating the national trader interface.
17. With respect to submissions, amendments, invalidation, processing, storage of the particulars of the entry summary declarations and notifications of arrival, as well as exchange of information between the Contracting Parties and economic operators, economic operators may choose to use the national trader interface, where developed, or the harmonised trader interface.
18. The national trader interface, where developed, shall interoperate with the ICS2 common repository.
19. When Norway develops a national trader interface, it shall inform the Union thereof.
20. A national entry system shall be used by the customs authorities of the Contracting Parties for exchange of entry summary declaration particulars extracted from the declarations referred in Article 9c of this Protocol, exchange of information and notifications with the common repository for information regarding arrival of sea-going vessel or an aircraft, information regarding presentation of goods, processing of risk analysis requests, exchange and processing of information regarding risk analysis results, of control recommendations, of control decisions and of control results.
21. The national entry system shall also be used in the cases where a customs authority of a Contracting Party requests further information from the economic operators and receives information thereof.
22. The national entry system shall interoperate with the common repository.
23. The national entry system shall interoperate with systems developed at national level for retrieving information referred to in paragraph 20.

Article 12

Functioning of the Import Control System 2 and Training in the use thereof

1. The common components shall be developed, tested, deployed and managed by the Union. The national components shall be developed, tested, deployed and managed by Norway.
2. Norway shall ensure that the national components are interoperable with the common components.
3. The Union shall perform the maintenance of the common components and Norway shall perform the maintenance of its national components.
4. The Contracting Parties shall ensure uninterrupted operation of the electronic systems.
5. The Union may change the common components of the electronic systems to correct malfunctions, to add new functionalities or alter existing ones.
6. The Union shall inform Norway of changes and updates to the common components.
7. Norway shall inform the Union of changes and updates to the national components that may have repercussions on the functioning of the common components.
8. The Contracting Parties shall make the information on the changes and updates to the electronic systems pursuant to paragraphs 6 and 7 publicly available.
9. In the case of temporary failure of the ICS2 the business continuity plan determined by the Contracting Parties shall apply.
10. The Contracting Parties shall inform each other of the unavailability of the electronic systems resulting from a temporary failure.

11. The Union shall support Norway on the use and functioning of the common components of the electronic systems by providing the appropriate training material.

Article 13

Uniform User Management and Digital Signature platform

1. A Uniform User Management and Digital Signature (or "UUM&DS") platform shall enable the communication between the identity and access management systems of the Contracting Parties referred to in paragraph 6 for the purposes of providing secure authorised access to the electronic systems to the Contracting Parties' officials and economic operators.

2. The UUM&DS platform shall consist of the following common components:

- (a) an access management system;
- (b) an administration management system.

3. The UUM&DS platform shall be used to ensure the authentication and access verification of:

- (a) economic operators for the purposes of having access to ICS2;
- (b) the Contracting Parties' officials for the purposes of having access to the common components of the ICS2 and for the purposes of maintenance and management of the UUM&DS platform.

4. The Contracting Parties shall set up the access management system to validate the access requests submitted by economic operators within the UUM&DS platform by interoperating with the Contracting Parties' identity and access management systems referred to in paragraph 6.

5. The Contracting Parties shall set up the administration management system to manage the authentication and authorisation rules for validating the identification data of economic operators for the purposes of allowing access to the electronic systems.

6. The Contracting Parties shall set up an identity and access management system to ensure:

- (a) a secure registration and storage of identification data of economic operators;
- (b) a secure exchange of signed and encrypted identification data of economic operators.

Article 14

Data Management and Ownership and Security

1. The Contracting Parties shall ensure that the data registered at national level corresponds to the data registered in the common components and is kept up to date.

2. By derogation from paragraph 1 the Contracting Parties shall ensure that the following data corresponds to and is kept up to date with data in the common repository of ICS2:

- (a) data registered at national level and communicated from the national entry system to the common repository;
- (b) data received from the common repository to the national entry system.

3. The data in the ICS2 common components that is communicated to or registered in the shared trader interface by an economic operator may be accessed or processed by that economic operator.

4. The data in the ICS2 common components:

- (a) communicated to a Contracting Party by an economic operator through the harmonised trader interface into the common repository may be accessed and processed by that Contracting Party in the common repository. Where needed, that Contracting Party may also access the information registered in the harmonised trader interface;
- (b) communicated to or registered in the common repository by a Contracting Party may be accessed or processed by that Contracting Party;

- (c) referred to in points (a) and (b) of this paragraph may also be accessed and processed by the other Contracting Party where the latter is involved in the risk analysis and/or control process to which the data relates in accordance with Articles 9c and 9e of this Protocol and this Annex;
 - (d) may be processed by the Commission in cooperation with the Contracting Parties for the purposes referred to in Article 1(1)(c) and Article 11(6). The results of such processing may be accessed by the Commission and the Contracting Parties.
5. The data in the ICS2 common component that is registered in the common repository by the Union may be accessed by the Contracting Parties. That data may be processed by the Union.
6. The Union shall be the system owner of the common components.
7. Norway shall be the system owner of its national components.
8. The Union shall ensure the security of the common components while Norway shall ensure the security of its national components.
9. For those purposes, the Contracting Parties shall take, at least, the necessary measures to:
- (a) prevent any unauthorised person from having access to installations used for the processing of data;
 - (b) prevent the entry of data and any consultation, modification or deletion of data by unauthorised persons;
 - (c) detect any of the activities referred to in points (a) and (b).
10. The Contracting Parties shall inform each other of any activities that might result in a breach or a suspected breach of the security of the electronic systems.
11. The Contracting Parties shall establish security plans concerning all systems.
12. The data registered in the components of the ICS2 shall be stored for a minimum of three years after its registration. The Contracting Parties may exceed that three-year period where required by relevant national legislation.

Article 15

Processing of personal data

For ICS2 and UUM&DS in relation to the processing of personal data therein,

1. Norway and the EU Member States shall act as controllers in compliance with the provision of Article 14 of the Agreement.
2. The Commission shall act as processor and shall comply with the obligations imposed on it in that respect pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council ⁽⁶⁾, except that, where processing the data for monitoring and evaluating the implementation of the common security and safety risk criteria and standards and of the control measures and priority control area, the Commission shall act as a joint controller.

Article 16

Participation in the development, maintenance and management of ICS2

The Union shall enable the experts from the EFTA State concerned to participate as observers for items concerning the development, maintenance and management of the ICS2 in meetings of the Customs Expert Group and the respective working groups. The Union shall decide on a case-by-case basis on the participation of the experts from the EFTA State concerned in meetings of the working groups in which only a limited number of EU Member States are represented and which report to the Customs Expert Group.

⁽⁶⁾ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

TITLE III

Article 17

Financing Arrangements concerning the responsibilities, commitments and expectations upon the implementation and operation of the ICS 2

Regarding the extension of the use of ICS2 to Norway, and in consideration of Chapter IIa and this Annex, these Financing Arrangements (hereinafter referred to as "the Arrangement") define the elements of collaboration between the Contracting Parties, related to the ICS2.

- (a) The Commission will develop, test, deploy, manage and operate the ICS2 central components consisting of a shared trader interface and a common repository (hereinafter "ICS2 central components"), including the applications and services required for their operation and interconnection with the IT systems in Norway such as TAPAS, UUM&DS, CCN2ng middleware, and commits to make them available to Norway.
- (b) Norway will develop, test, deploy, manage and operate the ICS2 national components.
- (c) Norway and the Commission agree to share the development and one-off costs of ICS2 central components as well as the operational costs of ICS2 central components, related applications and services required for their operation and interconnection, as follows:
 - (1) Part of the ICS2 development costs of central components will be invoiced by the Commission to Norway in accordance with letters d) and e). The development costs cover the software development of the central components and the acquisition and installation of the related infrastructure (hardware, software, hosting, licences, etc.). The allocation formula concerns 4% of all costs for the mentioned services.
 - (2) The maximum development costs will be capped at EUR 550 000 (five hundred and fifty thousand) per release.
 - (3) Part of the ICS2 and TAPAS operational costs will be invoiced by the Commission to Norway in accordance with letters f), g) and h). The operational costs cover the conformance testing, the maintenance of the infrastructure (hardware, software, hosting, licences, etc.), of the ICS2 central components and of the related applications and services required for their operation and interconnection (quality assurance, helpdesk and IT service management). The allocation formula concerns 4% of all costs for the mentioned services.
 - (4) The operational costs related to the use of ICS2 for Norway shall not exceed the maximum amount of EUR 450 000 (four hundred and fifty thousand) per year.
 - (5) The development and operational costs of national component(s) will be entirely borne by Norway.
 - (6) Norway shall be kept informed of the planned evolution of the costs and shall be informed of the main elements for the development of ICS2 that might have an impact on those costs.
- (d) Norway agrees to participate in the costs for the development and conformance testing of ICS2 central components incurred prior to the implementation of the Agreement. For that purpose:
 - (1) the Commission will inform Norway of the estimated amount of necessary contribution from the years prior to the implementation of the Agreement.
 - (2) By 15 May each year, starting from 15 May 2021, the Commission will request Norway to pay its contribution to those prior costs in equal instalments over the first four years of use of ICS2.
- (e) Norway agrees to participate in the development costs of the ICS2 central components. For that purpose:
 - (1) Norway agrees to pay its participation in the development costs of release 1, release 2 and release 3 of the ICS2.
 - (2) By 15 May each year, starting from 15 May 2021, the Commission will request Norway to pay its contribution to the development of the latest release on the basis of a duly documented debit note issued by the Commission.

- (f) Norway agrees to participate in the operational costs of the ICS2 central components. For that purpose:
- (1) By 31 July each year, starting from 31 July 2021, the Commission will inform Norway of the estimated operational costs for the following year and send to Norway the estimated amount of necessary contribution for the next year in writing. Norway will be informed in the same way and at the same time as the Commission informs each one of the other members of ICS2, as well as of the main aspects of the development of the ICS2.
 - (2) by 15 May 2021 only, the Commission will request Norway to pay its annual contribution for the operational costs of year 2020 amounting to EUR 110 000, as well as the estimated annual contribution for 2021 amounting to EUR 280 000. By 15 May each year, starting from 15 May 2022, the Commission will request Norway to pay its annual contribution for that year plus the amount of the balance (negative or positive) of the previous year on the basis of a duly-documented debit note issued by the Commission;
 - (3) By 31 January each year, starting from 31 January 2022,
 - The Commission will clear the accounts relating to the past annual costs of operating the ICS2 and TAPAS on the basis of the sum already paid by Norway as against actual costs incurred by the Commission and will provide Norway with a statement of account containing a breakdown of costs identifying the different services and the supply of software; and
 - provide Norway with the actual annual costs, i.e. real operational costs, for the past year. The Commission will calculate the actual and estimated costs in accordance with its contracts with contractors established under the current procedures for the award of contracts.

The balance (negative or positive) between the actual costs and the estimated amount of the previous year will be calculated and communicated to Norway via a statement of account from the Commission. The statement of account will include the estimated annual amount for the contribution, plus the amount of the balance (negative or positive), resulting in a net amount that the Commission will invoice to Norway via the annual debit note.
- (g) The payment by Norway will take place after the issuing date of the debit note. All payments must be made to the Commission bank account indicated on the debit note, within 60 days.
- (h) If Norway pays the amounts provided for in letter (c) later than the dates specified in letter (g), the Commission may charge interest on the arrears (at the rate applied by the European Central Bank to its operations in euro, published in the “C” series of the *Official Journal of the European Union*, on the day on which the deadline for repayment expires, plus one and a half points). The same rate will apply to payments to be made by the Union.
- (i) If Norway requests specific adjustments to or new IT products for the ICS2 central components, applications or services, the initiation and completion of those developments is subject to a separate, mutual agreement regarding resource needs and development costs.
- (j) All training materials created and maintained by the Contracting Parties shall be shared with all parties free of charge via electronic means. Norway may copy, distribute, display and perform the work and make derivative works based on the shared training materials
- (1) only if they give the author the credits in the manner specified in the shared training material;
 - (2) only for non-commercial purposes.
- (k) The Contracting Parties agree to acknowledge and fulfil their respective responsibilities in relation to the usage of the ICS2 central components as described in this Annex.
- (l) In the event of serious misgivings as to the proper functioning of this Annex or the ICS2 either Contracting Party may suspend the application of the Arrangement provided that the other Contracting Party has been notified in writing three months in advance.

TITLE IV

Exit summary Declaration*Article 18***Form and content of the exit summary declaration**

1. The exit summary declaration shall be lodged using a data processing technique. Commercial, port or transport documentation may be used, provided that it contains the necessary particulars.
2. The exit summary declaration shall contain the particulars laid down for such declaration in the columns A1 and A2 of Chapter 3 of Annex B of Commission Delegated Regulation (EU) 2015/2446 and comply with their respective formats, codes and cardinalities set out in Annex B of Commission Implementing Regulation (EU) 2015/2447. It shall be completed in accordance with the notes in those Annexes. The exit summary declaration shall be authenticated by the person who completed it.
3. The customs authorities shall allow the lodging of a paper-based exit summary declaration, or any other means replacing it as agreed between the customs authorities, only in one of the following circumstances:
 - (a) where the customs authorities' computerised system is not functioning;
 - (b) where the electronic application of the person lodging the exit summary declaration is not functioning, provided that the customs authorities apply the same level of risk management as that applied to exit summary declarations made using a data processing technique. The paper-based exit summary declaration shall be signed by the person who completed it. Such paper-based exit summary declarations shall be accompanied, where necessary, by loading lists or other appropriate lists, and shall contain the particulars referred to in paragraph 2.
4. Each Contracting Party shall define the conditions and procedures according to which the person lodging the exit summary declaration may modify one or more of the particulars of the declaration after lodging it.

*Article 19***Waiver from the obligation to lodge an exit summary declaration**

1. An exit summary declaration shall not be required in respect of the following goods:
 - (a) electrical energy;
 - (b) goods leaving by pipeline;
 - (c) items of correspondence;
 - (d) goods in postal consignments;
 - (e) goods for which an oral customs declaration or a declaration by simple crossing the border is permitted in accordance with the legislation of the Contracting Parties with the exception of pallets, containers, means of transport, as well as spare parts, accessories and equipment for such items, when carried under a transport contract.
 - (f) goods contained in travellers' personal luggage;
 - (g) goods covered by ATA and CPD Carnets;
 - (h) goods entitled to relief pursuant to the Vienna Convention on Diplomatic Relations of 18 April 1961, the Vienna Convention on Consular Relations of 24 April 1963 or other consular conventions, or the New York Convention of 16 December 1969 on Special Missions;
 - (i) weapons and military equipment brought out of the customs territory of a Contracting Party by the authorities in charge of the military defence of the Contracting Parties, in military transport or transport operated for the sole use of the military authorities;

- (j) the following goods brought out from the customs territory of a Contracting Party directly to offshore installations operated by a person established in a customs territory of the Contracting Parties:
 - (1) goods to be used for construction, repair, maintenance or conversion of the offshore installations;
 - (2) goods to be used to fit to or equip the offshore installations;
 - (3) provisions to be used or consumed on the offshore installations;
 - (k) goods moved under cover of the NATO form 302 provided for in the Convention between the Parties to the North Atlantic Treaty regarding the Status of their Forces, signed in London on 19 June 1951, or under cover of the EU form 302 provided for in point 51 of Article 1 of Commission Delegated Regulation (EU) 2015/2446;
 - (l) goods which are supplied for incorporation as part of or accessories in vessels or aircraft and for the operation of the engines, machines and other equipment of vessels or aircraft, as well as foodstuffs and other items to be consumed or sold on board;
 - (m) household effects as defined in the legislation of the respective Contracting Parties provided that they are not carried under a transport contract;
 - (n) goods dispatched from the customs territories of the Contracting Parties to Ceuta and Melilla, Heligoland, the Republic of San Marino, the Vatican City State, the municipalities of Livigno, and the Swiss customs exclaves of Samnaun and Sempoch;
 - (o) goods carried on vessels moving between ports of the Contracting Parties without any intervening call at any port outside the customs territories of the Contracting Parties;
 - (p) goods carried on aircraft moving between airports of the Contracting Parties without any intervening call at any airport outside the customs territories of the Contracting Parties.
2. An exit summary declaration shall not be required in the cases provided for in an international agreement concluded between a Contracting Party and a third country on security, subject to the procedure laid down in Article 9b(3) of this Protocol.
3. An exit summary declaration shall not be required by the Contracting Parties for goods in the following situations:
- (a) where a vessel that transports the goods between ports of the Contracting Parties is to call at a port outside the customs territories of the Contracting Parties and the goods are to remain loaded on board the vessel during the call at the port outside the customs territories of the Contracting Parties;
 - (b) where an aircraft that transports the goods between airports of the Contracting Parties is to call at an airport outside the customs territories of the Contracting Parties and the goods are to remain loaded on board the aircraft during the call at the airport outside the customs territories of the Contracting Parties;
 - (c) where, in a port or airport, the goods are not unloaded from the means of transport which carried them into the customs territories of the Contracting Parties, and which will carry them out of those territories;
 - (d) where the goods were loaded at a previous port or airport in the customs territories of the Contracting Parties where an exit summary declaration was lodged or a waiver from the obligation to lodge a pre-departure declaration was applicable and remain on the means of transport that will carry them out of the customs territories of the Contracting Parties;
 - (e) where goods in temporary storage or placed under the free zone procedure are transhipped from the means of transport that brought them to that temporary storage facility or free zone under the supervision of the same customs office onto a vessel, airplane or railway that will carry them out of the customs territories of the Contracting Parties, provided that the following conditions are fulfilled:
 - (1) the transhipment is undertaken within 14 days of the presentation of the goods in accordance with the legislation of the respective Contracting Party or in exceptional circumstances, within a longer period authorised by the customs authorities where the period of 14 days is not sufficient to deal with those circumstances;

- (2) information about the goods is available to the customs authorities;
- (3) the destination of the goods and the consignee do not change to the knowledge of the carrier;
- (f) where goods were brought into the customs territories of the Contracting Parties, but they were rejected by the competent customs authority and were immediately returned to the country of export.

Article 20

Place for lodging an exit summary declaration

1. The exit summary declaration shall be lodged with the competent customs office in the customs territory of the Contracting Party where the exit formalities for goods destined for third countries are carried out. However, a customs export declaration used as an exit summary declaration shall be lodged with the competent authority of the Contracting Party in whose customs territory the formalities related to the export to a third country are carried out. In either case, the competent office shall carry out the security and safety related risk analysis on the basis of the data included in the declaration as well as the security and safety customs controls that are deemed necessary.

2. When goods leave the customs territory of a Contracting Party to a third country through the customs territory of the other Contracting Party, and export formalities are followed by a transit procedure in accordance with the Convention on a Common Transit Procedure, NCTS shall be used to transmit the data referred to in Article 18 (2) to the competent authorities of the second Contracting Party.

In such a case, the customs office of the first Contracting Party shall make the results of its security and safety related customs controls available to the customs authority of the second Contracting Party where:

- (a) the risks are assessed by the customs authority as being significant and requiring customs control and the results of the control establish that the event triggering the risks has occurred; or
- (b) the control results do not establish that the event triggering the risks has occurred, but the customs authority concerned considers the threat to present a high risk elsewhere in the customs territories of the Contracting Parties; or
- (c) it is necessary for a uniform application of the rules in the Agreement.

The Contracting Parties shall exchange in the system referred to in Article 9e(3) of this Protocol the information on the risks mentioned under points (a) and (b) of this paragraph.

3. By derogation from paragraph 1, when goods leave the customs territory of a Contracting Party to a third country through the customs territory of the other Contracting Party, and the export formalities are not followed by a transit procedure in accordance with the Convention on a Common Transit Procedure, the exit summary declaration shall be lodged directly with the competent customs office of exit of the second Contracting Party where the goods are finally exited to a third country.

Article 21

Time limits for lodging an exit summary declaration

1. The exit summary declaration shall be lodged within the following time limits:

(a) in the case of maritime traffic:

- (1) for containerised cargo movements other than those referred to in points (2) and (3), at the latest 24 hours before the goods are loaded onto the vessel on which they are to leave the customs territories of the Contracting Parties;

- (2) for containerised cargo movements between the customs territories of the Contracting Parties and Greenland, the Faeroe Islands, Iceland or ports on the Baltic Sea, the North Sea, the Black Sea or the Mediterranean Sea, all ports of Morocco and the ports of the United Kingdom of Great Britain and Northern Ireland, with the exception of ports located in Northern Ireland, and ports of the Channel Islands and the Isle of Man, at the latest two hours before departure from a port in the customs territories of the Contracting Parties;
 - (3) for containerised cargo movements between the French overseas departments, the Azores, Madeira or the Canary Islands and a territory outside the customs territories of the Contracting Parties, where the duration of the voyage is less than 24 hours, at the latest two hours before departure from a port in the customs territories of the Contracting Parties;
 - (4) for movements not involving containerised cargo, at the latest two hours prior to departure from a port in the customs territories of the Contracting Parties;
 - (b) in the case of air traffic, at the latest 30 minutes prior to departure from an airport in the customs territories of the Contracting Parties;
 - (c) in the case of road and inland waterways traffic, at the latest one hour before the goods are to leave the customs territories of the Contracting Parties;
 - (d) in the case of rail traffic:
 - (1) where the train voyage from the last train formation station to the customs office of exit takes less than two hours, at the latest one hour before arrival of the goods at the place for which the customs office of exit is competent;
 - (2) in all other cases, at the latest two hours before the goods are to leave the customs territories of the Contracting Parties.
2. In the following situations, the time limit for lodging the exit summary declaration shall be that applicable to the active means of transport used to leave the customs territories of the Contracting Parties:
- (a) where the goods have arrived at the customs office of exit on another means of transport from which they are transferred before leaving the customs territories of the Contracting Parties (inter-modal transport);
 - (b) where the goods have arrived at the customs office of exit on a means of transport which is itself transported on an active means of transport when leaving the customs territories of the Contracting Parties (combined transportation).
3. The time limits referred to in paragraphs 1 and 2 shall not apply in the case of *force majeure*.
4. Notwithstanding paragraphs 1 and 2, each Contracting Party may decide on different time limits:
- in cases of the traffic referred to in Article 20(2) so that reliable risk analysis may be accrued out and shipments intercepted in order to carry out any security and safety related customs checks,
 - in the case of an international agreement on security between that Contracting Party and a third country, subject to the procedure referred to in Article 9b(3) of this Protocol.

ANNEX II

AUTHORISED ECONOMIC OPERATOR

TITLE I

Granting the status of authorised economic operator

Article 1

General provisions

The criteria for granting the status of authorised economic operator shall be the following:

- (a) the absence of any serious infringement or repeated infringements of customs legislation and taxation rules, including no record of serious criminal offences relating to the economic activity of the applicant;
- (b) the demonstration by the applicant of a high level of control of his/her operations and of the flow of goods, by means of a system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls;
- (c) financial solvency, which shall be deemed to be proven where the applicant has good financial standing, which enables him/her to fulfil his/her commitments, with due regard to the characteristics of the type of business activity concerned;
- (d) appropriate security and safety standards, which shall be considered as fulfilled where the applicant demonstrates that he/she maintains appropriate measures to ensure the security and safety of the international supply chain including in the areas of physical integrity and access controls, logistical processes and handling of specific types of goods, personnel and identification of his/her business partners.

Article 2

Compliance

1. The criterion laid down in Article 1(a) shall be considered to be fulfilled if:
 - (a) there is no decision taken by an administrative or judicial authority concluding that one of the persons described in point (b) has committed, over the last three years, a serious infringement or repeated infringements of customs legislation or taxation rules in relation to his/her economic activity; and
 - (b) none of the following persons has a record of serious criminal offence in relation to his/her economic activity including the applicant's economic activity, where applicable:
 - (1) the applicant,
 - (2) the employee(s) in charge of the applicant's customs matters, and
 - (3) the person(s) in charge of the applicant or exercising control over its management.
2. However, the criterion referred to in Article 1(a) may be considered to be fulfilled where the customs authority competent to take the decision considers an infringement to be of minor importance, in relation to the number or size of the related operations, and the customs authority has no doubt as to the good faith of the applicant.
3. Where the person referred to in paragraph 1(b)(3) of this Article, other than the applicant is established or has his/her residence in a third country, the customs authority competent to take the decision shall assess the fulfilment of the criterion referred to in Article 1(a) on the basis of records and information that are available to it.
4. Where the applicant has been established for less than three years, the customs authority competent to take the decision shall assess the fulfilment of the criterion referred to in Article 1(a) on the basis of the records and information that are available to it.

*Article 3***Satisfactory system of managing of commercial and transport records**

The criterion laid down in Article 1(b) shall be considered to be fulfilled if the following conditions are met:

- (a) the applicant maintains an accounting system which is consistent with the generally accepted accounting principles applied in the Contracting Parties where the accounts are held, allows audit-based customs control and maintains a historical record of data that provides an audit trail from the moment the data enters the file;
- (b) records kept by the applicant for customs purposes are integrated in the accounting system of the applicant or allow cross checks of information with the accounting system to be made;
- (c) the applicant allows the customs authority physical access to its accounting systems and, where applicable, to its commercial and transport records;
- (d) the applicant allows the customs authority electronic access to its accounting systems and, where applicable, to its commercial and transport records where those systems or records are kept electronically;
- (e) the applicant has an administrative organisation which corresponds to the type and size of business and which is suitable for the management of the flow of goods, and has internal controls capable of preventing, detecting and correcting errors and of preventing and detecting illegal or irregular transactions;
- (f) where applicable, the applicant has satisfactory procedures in place for the handling of licences and authorisations granted in accordance with commercial policy measures or relating to trade in agricultural products;
- (g) the applicant has satisfactory procedures in place for the archiving of its records and information and for protection against the loss of information;
- (h) the applicant ensures that relevant employees are instructed to inform the customs authorities whenever compliance difficulties are discovered and establishes procedures for informing the customs authorities of such difficulties;
- (i) the applicant has appropriate security measures in place to protect the applicant's computer system from unauthorised intrusion and to secure the applicant's documentation;
- (j) where applicable, the applicant has satisfactory procedures in place for the handling of import and export licences connected to prohibitions and restrictions, including measures to distinguish goods subject to the prohibitions or restrictions from other goods and measures to ensure compliance with those prohibitions and restrictions.

*Article 4***Financial solvency**

1. The criterion laid down in Article 1(c) shall be considered to be fulfilled where the applicant complies with the following:

- (a) the applicant is not subject to bankruptcy proceedings;
- (b) during the last three years preceding the submission of the application, the applicant has fulfilled its financial obligations regarding payments of customs duties and all other duties, taxes or charges which are collected on or in connection with the import or export of goods;
- (c) the applicant demonstrates on the basis of the records and information available for the last three years preceding the submission of the application that it has sufficient financial standing to meet its obligations and fulfil its commitments having regard to the type and volume of the business activity, including having no negative net assets, unless where they can be covered.

2. If the applicant has been established for less than three years, its financial solvency as referred to in Article 1(c) shall be checked on the basis of records and information that are available.

*Article 5***Security and safety standards**

1. The criterion laid down in Article 1(d) shall be considered to be fulfilled if the following conditions are met:
 - (a) buildings to be used in connection with the operations relating to the authorisation provide protection against unlawful intrusion and are constructed of materials which resist unlawful entry;
 - (b) appropriate measures are in place to prevent unauthorised access to offices, shipping areas, loading docks, cargo areas and other relevant places;
 - (c) measures for the handling of goods have been taken which include protection against the unauthorised introduction or exchange, the mishandling of goods and against tampering with cargo units;
 - (d) the applicant has taken measures allowing the clear identification of its business partners and to ensure, through implementation of appropriate contractual arrangements or other appropriate measures in accordance with the applicant's business model, that those business partners ensure the security of their part of the international supply chain;
 - (e) the applicant conducts in so far as national law permits, security screening on prospective employees working in security sensitive positions and carries out background checks of current employees in such positions periodically and where warranted by circumstances;
 - (f) the applicant has appropriate security procedures in place for any external service providers contracted;
 - (g) the applicant ensures that its staff having responsibilities relevant for security issues regularly participate in programmes to raise their awareness of those security issues;
 - (h) the applicant has appointed a contact person competent for security and safety related questions.
 2. Where the applicant is a holder of a security and safety certificate issued on the basis of an international convention, an International Standard of the International Organisation for Standardisation, or a European Standard of a European standardisation body, that certificate shall be taken into account when checking compliance with the criteria laid down in Article 1(d).
- The criteria shall be deemed to be met to the extent that it is established that the criteria for issuing that certificate are identical or equivalent to those laid down in Article 1(d).
3. Where the applicant is a regulated agent or a known consignor in the field of civil aviation security, the criteria laid down in paragraph 1 shall be deemed to be met in relation to the sites and the operations for which the applicant obtained the status of regulated agent or known consignor to the extent that the criteria for issuing the regulated agent or known consignor status are identical or equivalent to those laid down in Article 1(d).

TITLE II

Facilitation granted to authorised economic operators*Article 6***Facilitation granted to authorised economic operators**

1. Where an authorised economic operator for safety and security purposes lodges on his/her own behalf an exit summary declaration in the form of a customs declaration or a re-export declaration, no other particulars than those stated in those declarations shall be required.
2. Where an authorised economic operator for safety and security purposes lodges on behalf of another person who is also an authorised economic operator an exit summary declaration in the form of a customs declaration or a re-export declaration, no other particulars than those stated in those declarations shall be required.

Article 7

More favourable treatment regarding risk assessment and control

1. An authorised economic operator shall be subject to fewer physical and document-based security controls than other economic operators.
2. Where an authorised economic operator has lodged an entry summary declaration or has been authorised to lodge a customs declaration or a temporary storage declaration instead of an entry summary declaration or where an authorised economic operator has been authorised to use commercial, port or transport information systems for lodging the particulars of an entry summary declaration as referred to in Article 10(8) of the Agreement and Article 1(4) of Annex I the competent customs authority shall, where the consignment has been selected for physical control, notify the authorised economic operator of that fact. That notification shall take place before the arrival of the goods in the customs territory of the Contracting Parties.

That notification shall be made available also to the carrier if different from the authorised economic operator referred to in the first subparagraph, provided that the carrier is an authorised economic operator and is connected to the electronic systems relating to the declarations referred to in the first subparagraph.

That notification shall not be provided where it may jeopardise the controls to be carried out or the results thereof.

3. Where consignments declared by an authorised economic operator have been selected for physical or document-based control, those controls shall be carried out as a matter of priority.

On request from an authorised economic operator, the controls may be carried out at a place other than the place where the goods have to be presented to customs.

Article 8

Exemption from favourable treatment

The more favourable treatment referred to in Article 7 shall not apply to any security customs controls related to specific elevated threat levels or control obligations set out in other legislation.

However, customs authorities shall carry out the necessary processing, formalities and controls for consignments declared by an authorised economic operator as a matter of priority.

TITLE III

Suspension, annulment and revocation of the status of authorised economic operator

Article 9

Suspension of the status

1. A decision granting the status of authorised economic operator shall be suspended by the competent customs authority where:
 - (a) that customs authority considers that there may be sufficient grounds for annulling, or revoking the decision, but does not yet have all necessary elements to decide on the annulment, or revocation;
 - (b) that customs authority considers that the conditions for the decision are not fulfilled or that the holder of the decision does not comply with the obligations imposed under that decision, and it is appropriate to allow the holder of the decision time to take measures to ensure the fulfilment of the conditions or the compliance with the obligations;
 - (c) the holder of the decision requests such suspension because he/she is temporarily unable to fulfil the conditions laid down for the decision or to comply with the obligations imposed under that decision.

2. In the case referred to in points (b) and (c) of paragraph 1, the holder of the decision shall notify the customs authority of the measures he/she will take to ensure the fulfilment of the conditions or compliance with the obligations, as well as the period of time he/she needs to take measures.

When the economic operator concerned has, to the satisfaction of the customs authorities, taken the necessary measures to comply with the conditions and criteria that have to be met by any authorised economic operator, the issuing customs authority shall lift the suspension.

3. The suspension shall not affect any customs procedure already started before the date of suspension and not yet completed.

4. The holder of the decision shall be notified of its suspension.

Article 10

Annulment of the status

1. A decision granting the status of authorised economic operator shall be annulled if all the following conditions are fulfilled:

- (a) the decision was taken on the basis of incorrect or incomplete information;
- (b) the holder of the decision knew or ought reasonably to have known that the information was incorrect or incomplete;
- (c) if the information had been correct and complete, the decision would have been different.

2. The holder of the decision shall be notified of its annulment.

3. Annulment shall take effect from the date on which the initial decision took effect, unless otherwise specified in the decision in accordance with the customs legislation.

Article 11

Revocation of the status

1. A decision granting the status of authorised economic operator shall be revoked by the competent customs authorities where:

- (a) one or more of the conditions for taking that decision were not or are no longer fulfilled; or
- (b) upon application by the holder of the decision; or
- (c) the holder of the decision fails to take, within the prescribed period of time of the suspension referred to in points (b) and (c) of Article 9(1), the necessary measures to fulfil the condition laid down for the decision or to comply with the obligations imposed under the decision.

2. Revocation shall take effect on the day following its notification.

3. The holder of the decision shall be notified of its revocation.

TITLE IV

Article 12

Exchange of information

The Contracting Parties shall regularly inform each other of the identities of their authorised economic operators for the purposes of security, and include the following information:

- (a) the Trader Identification Number (TIN) in a format compatible with Economic Operator Registration and Identification (EORI) legislation;
- (b) the name and address of the authorised economic operator;
- (c) the number of the document granting the status of authorised economic operator;

- (d) current status (valid, suspended, revoked);
 - (e) periods of changed status;
 - (f) the date on which the decision and subsequent events (suspension and revocation) become effective;
 - (g) the authority which issued the decision.'
-

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)



Publications Office
of the European Union
L-2985 Luxembourg
LUXEMBOURG

EN