EUROPEAN
COMMISSION

Brussels, 23.2.2024
COM(2024) 86 final

ANNEX

ANNEX

to the

Proposal for a Council Decision

on the signing, on behalf of the Union, and provisional application of the Agreement between the European Union, of the one part, and the United States of America, of the other part, setting forth Security Procedures for the Launch of Galileo satellites from U.S. territory

AGREEMENT
between the
European Union
and the
United States of America
setting forth security procedures for the launch of Galileo satellites from U.S. territory

THE EUROPEAN UNION, hereinafter referred to as "the EU",

and

THE UNITED STATES OF AMERICA, hereinafter referred to as "the United States", hereinafter both referred to as "the Parties",

CONSIDERING the importance space technologies have for nations and their citizens in the domains of communication, remote sensing, navigation and national security,

CONVINCED of the need for the United States and the EU to cooperate so that the benefits of these important technologies can be fully achieved for all relevant applications,

RECALLING THAT Galileo is the EU's global navigation satellite system designed to provide free of charge positioning and timing information, for a wide range of sectors such as aviation, railways, shipping or telecoms,

CONSCIOUS THAT the import of European Union classified equipment into the territory of the United States for the purpose of satellite launches carries inherent security risks and merits appropriate security measures and cooperation between the United States and the EU,

CONSIDERING THAT the United States and the EU share the objective to prevent and protect against the misuse of space technologies, thereby strengthening their own security and providing their citizens with a high level of safety,

TAKING INTO ACCOUNT the strategic and scientific importance and the economic value of the Galileo satellites,

RECOGNISING the need to ensure protection of classified information and assets related to the launch of Galileo satellites,

CONSIDERING THAT the technical challenges accompanying satellite launches make the ongoing exchange of information and cooperation between the United States and the EU indispensable,

RECALLING the Agreement on the promotion, provision and use of Galileo and GPS satellite-based navigation systems and related applications between the United States of America, of the one part, and the European Community and its Member States, of the other part, signed at Dromoland Castle, Co. Clare, on 26 June 2004,

RECALLING the Agreement between the European Union and the Government of the United States of America on the security of classified information done at Washington on 30 April 2007 and in particular Article 19 thereof (hereinafter referred to as "the Security Agreement"), and its associated Security Arrangement for the protection of classified information exchanged between the EU and the United States of America, approved by an exchange of notes 26 July 2007 and 26 February 2008 (hereinafter referred to as "the Security Arrangement"),

CONSIDERING that the European Commission has entrusted the management of the launch service contracts for Galileo to the European Space Agency, hereinafter referred to as the "ESA", which is implementing the satellite launch campaigns for the European Union,

CONSIDERING the responsibilities of U.S. commercial Launch Service Providers as defined under U.S. law, regulation, policy, applicable licenses, and support arrangements, and the corresponding role and responsibilities of U.S. departments and agencies,

HAVE AGREED AS FOLLOWS:

Article 1
Scope

1. This Agreement shall apply to launches of Galileo satellites from the territory of the United States.

2. Both Parties acknowledge that EU classified equipment and documentation will be exported from the EU and imported into the United States, used in U.S. territory and re-exported to the EU. In order to protect the EU classified equipment and documentation, both Parties shall ensure, in close coordination with the Launch Service Provider, that all necessary and appropriate measures according to the terms of this Agreement are in place to control and protect such equipment and documentation.

3. Unless otherwise provided for in this Agreement or authorised by the European Commission following consultation by the Parties, the ESA Local Security Officer (hereinafter referred to as "ESA LSO"), his or her designees, and designees of the European Commission shall retain exclusive access to EU classified equipment and documentation during each launch campaign beginning with the arrival of such equipment and documentation on U.S. territory and ending with the removal from U.S. territory.

4. In the event EU classified information (hereinafter referred to as "EUCI") is released to or otherwise received by the United States government or by authorised third parties referenced in Article 5(4) or any other third parties mutually decided upon by the Parties, the terms of the Security Agreement and the terms included herein shall apply to and govern the protection of such EUCI, irrespective of the providing European entity.

Article 2
Definitions

For the purposes of this Agreement,

1. ‘EU classified information’ means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the EU or of one or more of its Member States. EUCI may be in oral, visual, electronic, magnetic or documentary form, or in the form of material, including equipment and technology.

2. ‘EU classified equipment and documentation’ means equipment and documentation containing EUCI.

3. ‘EU Protected Assets’ means any object or material on a Launch Base that is imported into the territory of the United States for the purpose of launch of a Galileo satellite, including but not limited to EU classified equipment and documentation.

4. ‘Secure Zones’ means areas at the Launch Base for storage and handling of EU Protected Assets, in accordance with the EU’s contractual arrangement with the Launch Service Provider and the Launch Service Provider’s support arrangements with the Launch Base.

5. ‘Launch Base’ means a particular location or locations on U.S. government property with facilities for assembling the launch vehicle, handling its fuel, preparing a spacecraft for launch, launching and monitoring of launches, which is located within the territory of the United States, and from which the launch of the Galileo satellites is to take place.

6. ‘Commercial Payload Processing Facility’ means a facility for preparing a spacecraft and payload for launch, which is located within the territory of the United States on private property outside of the Launch Base.

7. ‘Security Incident’ means any event that may result in unauthorised access, use, disclosure, modification or destruction of information, documentation, equipment or interference with system operations of EU Protected Assets.

8. ‘Launch Service Provider’ means the U.S. organisation contracted by the European Commission to perform the launch of the Galileo satellites.

9. ‘Galileo’ means the EU’s autonomous civil global navigation satellite system (GNSS) under civil control, which consists of a constellation of satellites, control centres and a global network of ground stations, offering positioning, navigation and timing services including security needs and requirements.

10. ‘Galileo satellite’ means a spacecraft pertaining to the Galileo system that is imported into the territory of the United States for the purposes of launch.

11. ‘Galileo satellite debris’ means any Galileo satellite or its part, including fragments and elements thereof, which are found on the territory of the United States or in U.S. territorial waters or international waters following a mishap or accident involving the Galileo satellite.

12. ‘European Space Agency’ is an intergovernmental organisation, established by the Convention for the establishment of a European Space Agency opened for signature in Paris on 30 May 1975 and entered into force on 30 October 1980. In accordance with Article 28(4) of Regulation (EU) 2021/ 696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme (hereinafter the “EU Space Regulation”), the European Union has entrusted to ESA tasks relating to the implementation of the Union Space Programme, including procurement and execution of specific launch service contracts, which ESA performs for the European Union.

13. ‘European Union Agency for the Space Programme’ (hereinafter referred to as “EUSPA”) is the EU Agency established by the EU Space Regulation, which is entrusted by the European Commission with the management and the exploitation of the Galileo component of the EU Space Programme.

14. ‘ESA Local Security Officer’ means the ESA official designated by the European Commission, who is responsible for the security of the EU’s Galileo launch campaigns.

15. ‘ESA LSO designees’ means ESA personnel and ESA contractors designated by the ESA LSO in writing to carry out a specific role, responsibility, or task on their behalf. The designation is restricted to a specific task and is not authorisation for the designee to act on behalf of the ESA LSO in a general sense.

16. ‘Designees of the European Commission’ means EU including EUSPA staff and EU Member State experts designated by the European Commission in writing to carry out a specific role, responsibility, or task on its behalf. The designation is restricted to a specific task and is not authorisation for the designee to act on behalf of the European Commission in a general sense.

Article 3
Import procedures

1. The import of EU Protected Assets to the territory of the United States shall be subject to the laws of the United States, including laws administered or enforced by U.S. Customs and Border Protection (CBP). CBP shall, in accordance with applicable law and policy, exercise discretion regarding whether inspection of the subject items is necessary.

2. The EU, in coordination with the Launch Service Provider, shall provide to the relevant U.S. agencies all information required under U.S. law to enable customs clearance of EU Protected Assets, including satisfaction of applicable licensing requirements. The United

States shall provide the European Commission with information on the anticipated customs clearance procedures.

3. In the event that CBP identifies a need to inspect a Galileo satellite or other EU Protected Assets, the CBP Point of Contact designated pursuant to Article 9 shall contact the ESA LSO and, to the extent practicable, ensure that the ESA LSO and/or his/her designees are present for such inspection. Any such customs inspection shall be conducted in accordance with applicable U.S. law, in a Secure Zone or other mutually designated facility on the Launch Base with security commensurate with the nature of the item(s) being inspected, and shall be carried out only to the extent necessary to ensure conformity with U.S. law.

4. The ESA LSO may make a request to CBP that any inspection be paused to enable prior bilateral consultation between the European Commission and the U.S. Department of State. Absent immediate danger to human life or United States' national security, CBP would expect to accommodate such a request.

Article 4
Protection of the Launch Base Secure Zones and EU Protected Assets

1. In a manner consistent with U.S. law, policies, procedures and support arrangements with the Launch Service Provider:

   a. The United States shall take all necessary and appropriate steps to protect the Launch Base against any intrusion, including those areas containing a Secure Zone.

   b. The United States shall take all necessary and appropriate measures to prevent damage, alteration and tampering of Galileo satellites during the launch campaign beginning with their arrival on U.S. territory and ending with removal from U.S. territory.

   c. United States shall confirm, upon request from the European Commission, the status of the facility security clearance of the Launch Service Provider and owner/operator of the Commercial Payload Processing Facility under United States domestic law pertaining to the storage of classified equipment and documentation. The United States shall notify the European Commission of any change in status previously confirmed.

   d. Subject to Articles 3.3, 5.4 and 6.3, the United States shall not access or inspect EU Protected Assets on a Launch Base. The United States shall protect the Secure Zones from any form of unauthorised entry, eavesdropping or other forms of interference with the activities taking place at the Secure Zones.

   e. United States government and supporting contractor personnel may access and inspect a Secure Zone located on a Launch Base for the limited purpose of confirming compliance with safety, security, and environmental requirements, for criminal law enforcement, or as otherwise provided for in Article 5. In the event of such access or

inspection, United States government and supporting contractor personnel shall provide reasonable notice to facilitate timely access to the Secure Zone by the ESA LSO or his/her designees, and shall not exclude the ESA LSO or his/her designees from a Secure Zone, except in limited cases of urgent and immediate threat to human life or risk to United States national security or for criminal law enforcement purposes. In such cases, United States government personnel shall nonetheless keep the ESA LSO or if not available his/her designees appropriately informed and make every effort to ensure uninterrupted operation of EU video systems authorised under contract with the Launch Service Provider.

f. The United States shall not impede the EU's use of duly imported telecommunications encryption equipment in Secure Zones on the Launch Base or Commercial Payload Processing Facility. The EU shall use such equipment solely through the Launch Service Provider's or Commercial Payload Processing Facility's communications network unless otherwise authorised by the United States.

2. The United States shall keep the ESA LSO informed through the Launch Service Provider prior to any decision to evacuate any area of the Launch Base related to the EU launch. To the extent practicable in such circumstances, the EU shall be permitted to post a guard 24/7 in or around the Secure Zones and continue monitoring the Secure Zones remotely via EU video systems authorised under contract with the Launch Service Provider.

3. Prior to the deployment or storage of the EU classified equipment and documentation in a Secure Zone located on a Launch Base or in a Commercial Payload Processing Facility, the United States shall, following a request from the European Commission, notify it in writing that all necessary and appropriate security measures are in place.

4. The provisions set forth in this Article apply principally to activities and EU Protected Assets at a Launch Base and, unless otherwise provided in this Article, do not extend to activities and EU Protected Assets at a Commercial Payload Processing Facility. EU activities and EU Protected Assets at a Commercial Payload Processing Facility are governed primarily by contractual agreements between the EU, the Launch Service Provider and the owner/operators of such a facility.

5. The EU shall provide to the United States in writing the list of EU classified equipment and documentation involved in a launch campaign and the list of EU Protected Assets.

6. The Parties shall designate jointly in writing the Launch Base, Commercial Payload Processing Facility and the Secure Zones that may be used by the EU during each launch campaign.

Article 5

Security investigation

1. In the case of a suspected Security Incident, the ESA LSO shall, if he/she considers appropriate and following a clarification meeting with the security officer of the Launch Service Provider, report the Security Incident to the United States Launch Base Security Authority for further investigation. The ESA LSO shall also report the Security Incident to the U.S. Department of State.

2. The U.S. Launch Base Security Authority, in coordination with the Launch Service Provider, ESA LSO and other applicable organisations, shall investigate any Security Incident reported by the ESA LSO.

3. When an investigation has been completed, the United States shall submit a full report to the European Commission, consistent with Article 25(b) of the Security Arrangement, and identify any remedial or corrective action to be taken as appropriate.

4. United States government personnel or other federal or state authorities, Launch Service Provider personnel, and their respective supporting contractors, holding requisite security clearances, may access or inspect EU Protected Assets only in case of investigation following the Security Incident reported by the ESA LSO to the United States Launch Base Security Authority. Such access shall be allowed exclusively for investigative purposes and after prior authorisation by the European Commission as conveyed by the ESA LSO to the U.S. Launch Base Security Authority. The U.S. Launch Base Security Authority, or other appropriate United States authority, shall in turn authorise access to EUCI to appropriate federal, state and Launch Service Provider personnel, and their respective contractors, consistent with the European Commission authorisation.

5. Consistent with Article 3.3 of the Security Agreement, EU classified information released by the European Commission, designees of the European Commission, or by the ESA LSO, including his/her designees, to the United States for the purposes of implementation of this Agreement, or that the United States otherwise received, shall be protected by the United States in a manner at least equivalent to that afforded to it by the European Union. Annex A to this agreement shall apply to information stamped, marked, or designated "RESTREINT UE/EU RESTRICTED" that is released to or otherwise received by the United States.

6. The Parties recognise that a Security Incident arising at a Commercial Payload Processing Facility or in transit would pose complex and unique jurisdictional challenges. In such a circumstance, the United States Launch Base Security Authority would use its best efforts to facilitate the investigation of any such incident with the relevant parties, including the EU, the Launch Service Provider, the Commercial Payload Processing Facility owner/operator, and appropriate U.S. federal and state authorities.

Article 6
Recovery of Galileo satellite debris

1. In case of a mishap or accident that leads to the destruction of the Galileo satellite, the United States shall, in a manner consistent with U.S. law, policies, procedures and U.S. support arrangements with the Launch Service Provider, authorise the ESA LSO, his/her designees, and the designees of the European Commission as communicated by its point of contact specified in Article 9 to:

   a. Participate in the search and to collect Galileo satellite debris at the debris locations.

   b. Store Galileo satellite debris at a Secure Zone under continuous supervision of the ESA LSO.

   c. Transport the Galileo satellite debris to the territory of the European Union.

2. During the recovery operations, each of the Parties shall notify without delay to the other Party whenever made aware of the location of Galileo satellite debris, outside of the defined search area, to the extent practical prior to its physical removal from the debris locations.

3. United States government and Launch Service Provider personnel and their supporting contractors may inspect recovered Galileo satellite debris only for investigative purposes. In doing so they shall accommodate the presence of the ESA LSO. Any inspection of recovered Galileo satellite debris beyond a visual inspection should take place only after consultations between the Parties.

4. The ESA LSO may request to the Federal Aviation Administration (FAA) Point of Contact designated pursuant to Article 9 that any planned inspection of Galileo satellite debris be paused to enable prior bilateral consultation between the European Commission and the U.S. Department of State. Absent immediate danger to human life or safety, FAA would expect to accommodate such a request.

Article 7
Registration

1. With respect to each Galileo satellite launched from U.S. territory in connection with this Agreement, the EU shall ensure the provision of information about the space object to the Secretary-General of the United Nations, consistent with the Convention on the Registration of Objects Launched into Outer Space, done on November 12, 1974 (Registration Convention).

2. The Parties agree that the United States shall not be responsible for registering Galileo satellites in accordance with the Registration Convention, and that the United States has no jurisdiction or control over such objects in outer space.

Article 8
Liability

1. In the event the Galileo satellite, or a component part thereof, causes damage giving rise to one or more claims for compensation made against the United States under international law:

   a. The United States may seek to substitute the European Union in place of the United States in whatever forum such a claim is brought. The EU shall facilitate such efforts.

   b. If such substitution is not successful, the EU agrees to hold the United States harmless and indemnify the United States in relation to any financial obligation arising from the settlement or adjudication of such claims. The Parties shall coordinate on the defence to such claims.

   c. In the event of a dispute or potential claim, the United States shall notify the EU promptly in writing, providing all relevant details.

   d. If the United States elects to settle the claim, it should obtain the EU's written consent before agreeing to the settlement. The EU shall be responsible for indemnifying the United States for the settlement amount only if it granted its consent to the settlement.

   e. The Parties agree to consult at all stages, as appropriate, on the handling and disposition of any such claims.

2. For purposes of this article, the term "damage" means loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical.

3. Nothing in this Agreement is to be construed as a waiver of the sovereign immunity of the United States or of any other privileges or immunities derived from customary international law, from treaties and agreements in force between the United States and the European Union, or from any other international legal obligations.

Article 9
Points of Contact

1. To facilitate implementation of this Agreement, the Parties shall designate and provide to the other in writing operational points of contact, and their contact information, for the entities set out in paragraphs 2 and 3.

2. On the part of the European Union:

- European Commission
- European Space Agency Local Security Officer
- European Space Agency
- European Union Agency for the Space Programme
- Launch Service Provider
- Satellite Manufacturer.

3. On the part of the United States:

- Launch Base Security Authority
- Launch Base Senior Authority
- Customs and Border Protection
- Federal Aviation Administration.

Article 10
Dispute settlement

Any disputes between the Parties arising under or relating to this Agreement shall be settled solely through consultations between the Parties.

Article 11
Other agreements

Nothing in this Agreement shall alter existing agreements or arrangements between the Parties.

Article 12
Entry into force and termination

1. This Agreement shall enter into force on the day following the date of receipt of the last note in an exchange of diplomatic notes whereby the Parties have notified each other of the completion of their respective internal procedures for the entry into force of this Agreement and shall remain in force until 1 January 2027.

2. The European Union and the United States may apply this Agreement provisionally, in whole or in part, in accordance with their respective internal procedures and legislation. The provisional application shall begin on the day following the date on which:

   a) the European Union has notified the United States of the parts of this Agreement that it proposes to provisionally apply; and
   b) the United States confirms its agreement to the parts of the Agreement that shall be provisionally applied.

3. Either Party may notify in writing the other Party of its intention to terminate this Agreement. The termination shall take effect eight months after the date of receipt of the notification.

4. This Agreement may be amended or extended by mutual written agreement of the Parties.

5. Annex A, which sets forth measures to protect RESTREINT UE/EU RESTRICTED information, constitutes an integral part of this Agreement.

Article 13
Authentic Text

The signed English text of this Agreement shall be the authentic text. This Agreement is drawn up by the EU also in the Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages.

IN WITNESS WHEREOF, the undersigned, being duly authorised thereto by their respective Authorities, have signed this Agreement.

Done at (place) this (…) day of (year), in two originals in the English language.

For the European Union

For the United States of America

Annex A

Measures to protect RESTREINT UE/EU RESTRICTED information

RESTREINT UE/EU RESTRICTED information may be in oral, visual, electronic, magnetic or documentary form or in the form of material, including equipment or technology.

RESTREINT UE/EU RESTRICTED information may be recorded on any type of physical media.

1. Scope and responsibilities

The measures established in this Annex apply in the event the U.S. Launch Base Security Authority or other appropriate U.S. authority is provided or otherwise receives RESTREINT UE/EU RESTRICTED information under this agreement. The United States government or authorised third parties referenced in Article 5(4) or any other third parties mutually decided upon by the Parties accessing RESTREINT UE/EU RESTRICTED information under this Agreement are responsible for handling, storing and registering such information as described herein.

2. Clearance levels

RESTREINT UE/EU RESTRICTED information can only be accessed by authorised U.S. or third-party personnel having the required "need-to-know" as defined by the ESA LSO and the U.S. Launch Base Security Authority. Before access is granted, the individuals shall be briefed on the rules and the relevant security standards and guidelines for protecting RESTREINT UE/EU RESTRICTED information; and shall acknowledge their responsibilities for protecting this information.

A Personnel Security Clearance is not required for authorised U.S. or third-party personnel accessing RESTREINT UE/EU RESTRICTED information.

3. Handling

RESTREINT UE/EU RESTRICTED information may be handled in Secure Zones of the Launch Base as follows. Authorised U.S. or third-party personnel:

a) shall close the office door when handling RESTREINT UE/EU RESTRICTED information,
b) shall stow any RESTREINT UE/EU RESTRICTED information away or cover it should they receive a visitor,
c) shall not leave RESTREINT UE/EU RESTRICTED information visible when the office is unoccupied,
d) shall permanently turn away screens displaying RESTREINT UE/EU RESTRICTED information from windows and doors to prevent potential overlooking. Laptops used in meetings shall have anti-glare/privacy film on the screen.

RESTREINT UE/EU RESTRICTED information may be handled outside a Secure Zone, provided the person in possession of the information, (the "holder") has undertaken to comply with compensatory measures to protect it from access by unauthorised persons. The compensatory measures shall include at least the following:

a) RESTREINT UE/EU RESTRICTED information shall not be read in public places, nor left unattended in hotel rooms or vehicles,
b) RESTREINT UE/EU RESTRICTED information shall be kept at all times under the personal control of the holder,
c) RESTREINT UE/EU RESTRICTED information, while outside the Secure Zone, shall be carried in the manner described in Section 7 of this annex.
d) the documents shall be stowed in appropriate locked furniture when they are not being read or discussed,
e) the doors to the room shall be closed while the document is being read or discussed,
f) the details of the document shall not be discussed over the phone on a non-secured line, or on Voice/Video over IP via a connection which is not encrypted with an approved solution, or in an unencrypted email or in an email encrypted with non-approved solution,
g) mobile devices shall be shut down (or put in flight mode) while the document is being discussed,
h) the document may only be photocopied or scanned on stand-alone (not connected to any network) or accredited equipment,
i) the document shall only be handled and temporarily held outside a Secure Zone for the minimum time necessary,
j) the holder shall not throw the classified document away but shall return it for storage in a Secure Zone, or ensure it is destroyed in an approved shredder.

4. Storage

Hard copy RESTREINT UE/EU RESTRICTED information, including removable storage media with unencrypted information or with information encrypted with non-approved encryption solution, shall be stored in locked office furniture in a Secure Zone. It may be stored temporarily outside a Secure Zone provided the holder has undertaken to comply with relevant compensatory measures as provided for in the second part of point 2 above.

5. Distribution and release

Handling and management, including distribution of RESTREINT UE/EU RESTRICTED information, are a responsibility of the holder.

No release of RESTREINT UE/EU RESTRICTED information is allowed without the prior written consent of the European Commission.

6. Electronic transmission

Modalities of electronic transmission of RESTREINT UE/EU RESTRICTED information within internal U.S. government networks shall be decided on a case-by-case basis through consultation between the Parties.

7. Carrying RESTREINT UE/EU RESTRICTED information

Depending on the means available or the particular circumstances, RESTREINT UE/EU RESTRICTED information may be physically carried by hand in the form of paper documents or on removable storage media.

A consignment may contain more than one piece of RESTREINT UE/EU RESTRICTED information, provided the need-to-know principle is respected.

The packaging used shall ensure that the contents are covered from view. RESTREINT UE/EU RESTRICTED information shall be carried in opaque packaging, such as an envelope, an opaque folder or a briefcase. The outside of the packaging shall not bear any indication of the nature or classification level of its contents. If used, the inner layer of packaging shall be marked as RESTREINT UE/EU RESTRICTED. Both layers shall state the intended recipient's name, job title and address, as well as a return address in case delivery cannot be made.

Any security incidents involving RESTREINT UE/EU RESTRICTED information that is carried by authorised personnel or couriers shall be reported for subsequent investigation to the ESA LSO and the U.S. Launch Base Security Authority.

Removable storage media that are used to transport RESTREINT UE/EU RESTRICTED information shall be accompanied by a dispatch note, detailing the removable storage media containing the classified information, as well as all files contained on them, to allow the recipient to make the necessary verifications.

Only the necessary documents shall be stored on the media. For example, all the classified information on a single USB stick, should be intended for the same recipient. The sender shall bear in mind that large amounts of classified information stored on such devices may warrant a higher classification level for the device as a whole.

Only removable storage media bearing the appropriate classification marking shall be used to carry RESTREINT UE/EU RESTRICTED information. If the information is encrypted with an approved solution, there is no requirement to mark the removable media.

8. Reproduction

The reproduction of RESTREINT UE/EU RESTRICTED information is to be performed by the handler and limited to the strict operational needs, and provided the originator has not imposed any caveats. The handler of the document keeps a record on the distribution performed by him/her.

9. Destruction and deletion of RESTREINT UE/EU RESTRICTED information

Only level 4 of DIN 32757 and Level 5 of DIN 66399, or equivalent, shredders are suitable for destroying RESTREINT UE/EU RESTRICTED documents. The shred from approved shredders may be disposed of as normal office waste.

All media and devices containing RESTREINT UE/EU RESTRICTED information shall be properly sanitised when they reach the end of their lifetime. The electronic data shall be destroyed or erased from information technology resources and associated storage media in a manner that gives reasonable assurance that the information cannot be recovered. Sanitisation shall remove data from the storage device, and also remove all labels, markings and activity logs.

10. Declassification

RESTREINT UE/EU RESTRICTED information shall not be declassified without the permission of the European Commission.