# Cybersecurity:

## Contractual guidelines and other recommendations to maximise the legal security of the space activities

Avv. Francesco Amicucci

Thales Alenia Space Italia S.p.A.,
Rome, Italy

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

EUSPACE
European Union in Space
JEAN MONNET MODULE

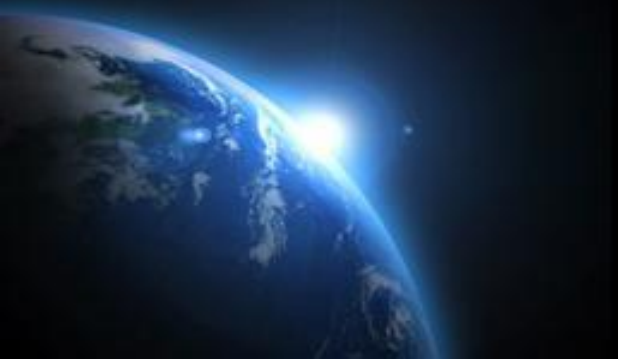
# Cybersecurity

UNIVERSITÀ DEGLI STUDI DI GENOVA

- The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

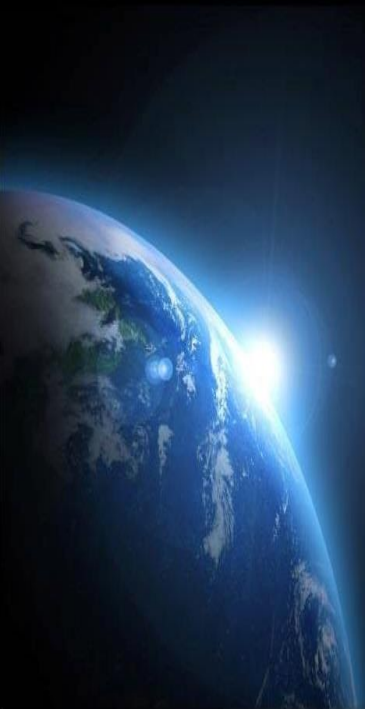
- Cybersecurity includes controlling physical access to system hardware, as well as protecting against harm that may be done via network access, malicious data and code injection.

- The field is of growing importance due to increasing reliance on computer systems, the Internet and wireless networks such as Bluetooth and Wi-Fi, and due to the growth of “smart” devices, including smartphones, televisions and the various tiny devices that constitute the Internet of Things.



EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



# Cybersecurity

Professionals working in the cybersecurity field can be known by some of the following terms:

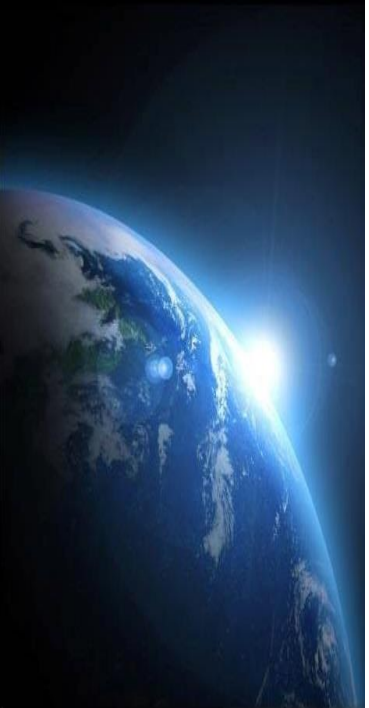
- White hat hacker – also known as an "ethical hacker" or penetration tester. They are professional hackers that break into systems and use exploits to access target systems for reasons pertaining to prevention of crime or hardening the security of a target.

- Black hat hacker – a criminal who breaks into systems and compromises security against the law.

- Grey hat hacker – someone who conducts black hat hacks for white hat hacker reasons.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



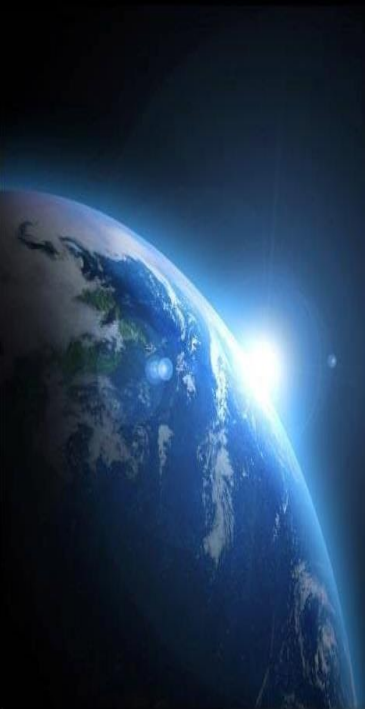
# Background

- Sharp increase in cyberthreats and cyberattacks
- Development of sector-specific regulations
- Increased customer focus on cyber issues
- New customer requests to incorporate specific contractual provisions to cover cyber risk

Need for the operators to define contractual cyber guidelines to curb risks.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



# Background

## Security Information Systems

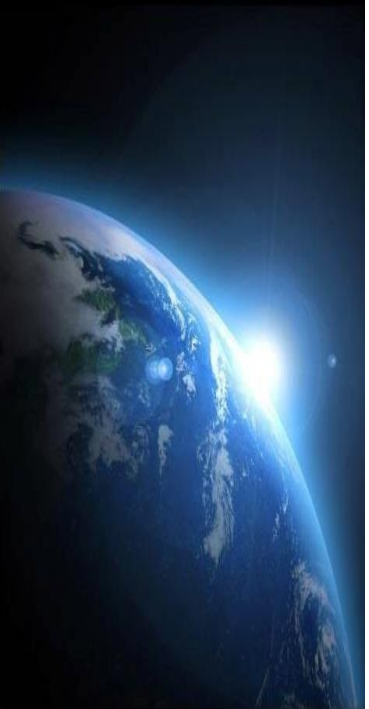
Present approach to cybersecurity is focused on how and what to do to prevent a security failure or accident and the way to behave when such failure/accident occurs.

The cybersecurity framework is issued by National Institute of Standards Technology that provides for the following processes:

- identify
- protect
- detect
- respond
- recover

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



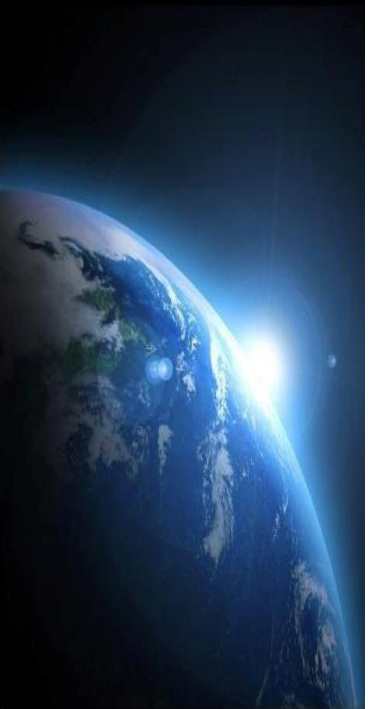
# Legislative and regulatory environment

- ☑ European Countries are working to standardise a legal corpus. EU has enacted, on Jul 6, 2016, the Directive 2016/1148 aimed at implementing precautionary measures for a common level of Networks and Information systems Security (namely NIS Directive).
- ☑ To date, the vast majority of these are sector-specific standards ➔ the main actors have launched discussions on the adoption of cybersecurity regulations, but these discussions have not yet concluded.

- ☑ Legislation seeks to strengthen corporate obligations to counter cyberattacks rather than strengthen sanctions against hackers.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



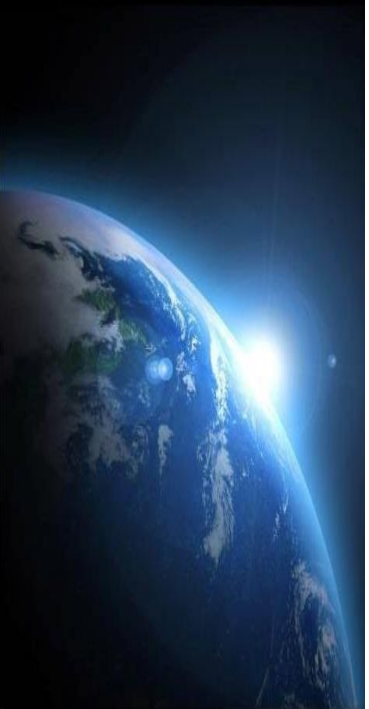
# Role of Government

- The role of the government is to make regulations to force companies and organizations to protect their systems, infrastructure and information from any cyberattacks, but also to protect its own national infrastructure such as the national power-grid.

- The question of whether the government should intervene or not in the regulation of the cyberspace is a very polemical one. Indeed, for as long as it has existed and by definition, the cyberspace is a virtual space free of any government intervention. Where everyone agrees that an improvement on cyber security is more than vital, is the government the best actor to solve this issue? Many government officials and experts think that the government should step in and that there is a crucial need for regulation, mainly due to the failure of the private sector to solve efficiently the cybersecurity problem.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

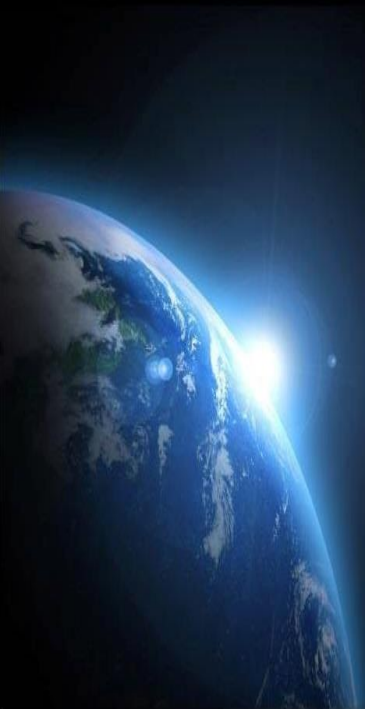


# Role of Government

- R. Clarke said during a panel discussion at the RSA Security Conference in San Francisco, he believes that the "industry only responds when you threaten regulation. If the industry doesn't respond (to the threat), you have to follow through." On the other hand, executives from the private sector agree that improvements are necessary, but think that the government intervention would affect their ability to innovate efficiently.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



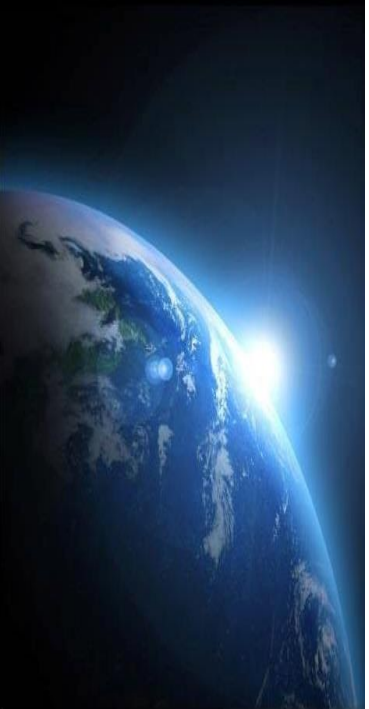
# International Actions

Many different teams and organizations exist, including:

- The Forum of Incident Response and Security Teams (FIRST) is the global association of CSIRTs. The US-CERT, AT&T, Apple, Cisco, McAfee, Microsoft are all members of this international team.
- The Council of Europe helps protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime.
- The purpose of the Messaging Anti-Abuse Working Group (MAAWG) is to bring the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations. France Telecom, Facebook, AT&T, Apple, Cisco, are some of the members of the MAAWG.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



# International Actions

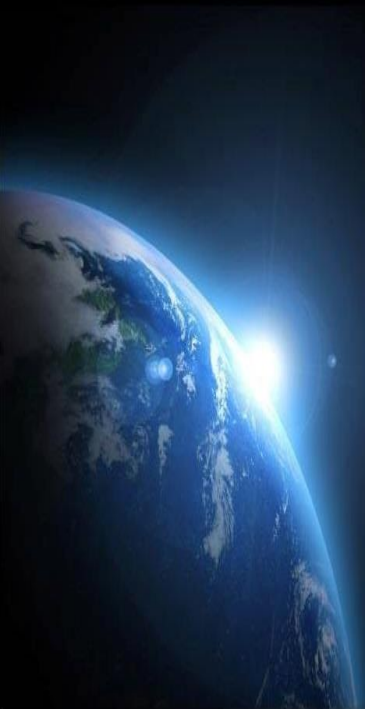
- ENISA : The European Network and Information Security Agency (ENISA) is an agency of the European Union with the objective to improve network and information security in the European Union.

**Europe**

- On 14 April 2016 the European Parliament and Council of the European Union adopted The General Data Protection Regulation (GDPR) (EU) 2016/67. GDPR, which became enforceable beginning 25 May 2018, provides for data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). GDPR requires that business processes that handle personal data be built with data protection by design and by default. GDPR also requires that certain organizations appoint a Data Protection Officer (DPO).

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



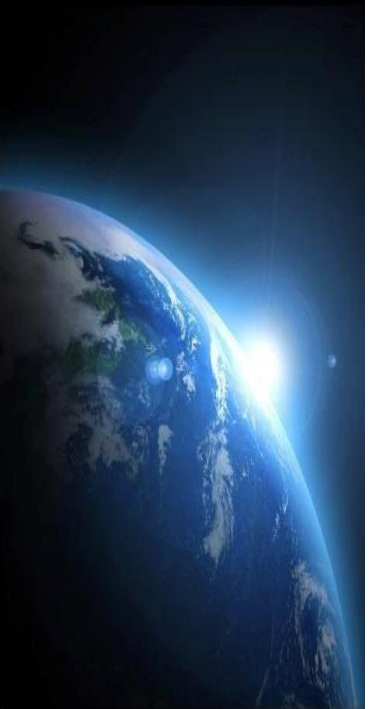
# International Actions

**Italy**

- Law n. 124 of August 3, 2007 «Information Systems for the Republic Security and new rules on secret matters» has stated that the Interministeral Committee for the Republic Safety (CISR) will adopt the necessary directives to consolidate the information activities aimed at protecting the tangible and instangible critical infrastructures with a specific focus on the cybernetic protection and the national informatic security.
- On February 17, 2017, lastly, through a Prime Minister Decree it was issued a directive indicating the patterns to be followed for the cybernetic protection and the national informatic security.
- The Prime Minister is responsible to lead the activities of CISR and its technical support. CISR is in charge to issue the National Plan for the cybernetic protection and the national informatic security.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

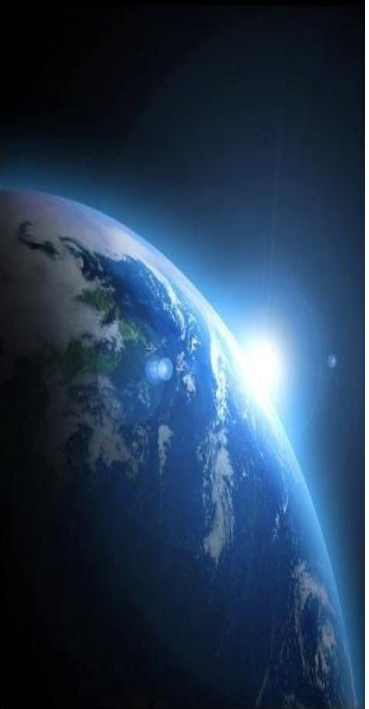


# Legislative and regulatory environment

- French Military Programming Act of 18 December 2013 (Articles L, 1332-6-1 to L, 1332-6-6 of the French Defence Code):
  - Enforcement by critical operators ("*opérateur d'importance vitale (OIV)*" in French) of rules expressly defined by decree for each sector;
  - Prompt notification to the Prime Minister of any security incidents affecting critical information systems ("*systèmes d'information d'importance vitale (SIIV)*" in French);
  - Possibility for the National Cybersecurity Agency of France ("*Agence nationale de la sécurité des systèmes d'information (ANSSI)*" in French) to carry out SIIV checks in order to verify their level of security;
  - Obligation to put in place measures to respond to major crises.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



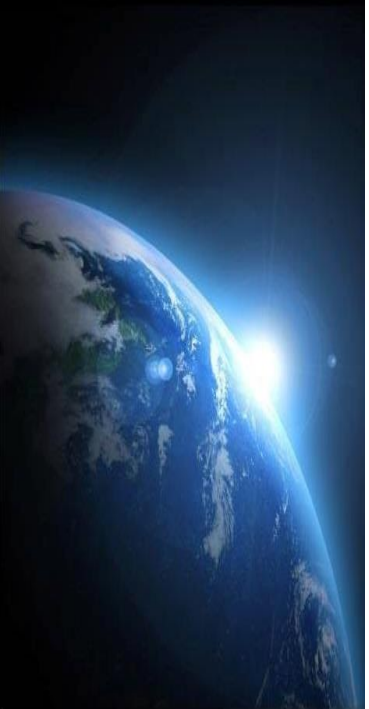
# Legislative and regulatory environment

- Regulation of 11 August 2016 laying down the security rules and procedures for the reporting of critical information systems and security incidents in the “Air transport” and “Land transport” critical activities subsectors:

- Obligation to register SIIVs
- Obligation by SIIVs to maintain a state of operational security (“*Maintien en condition de sécurité (MCS)*” in French)
- Obligation to set up a system for the detection and prevention of incidents

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



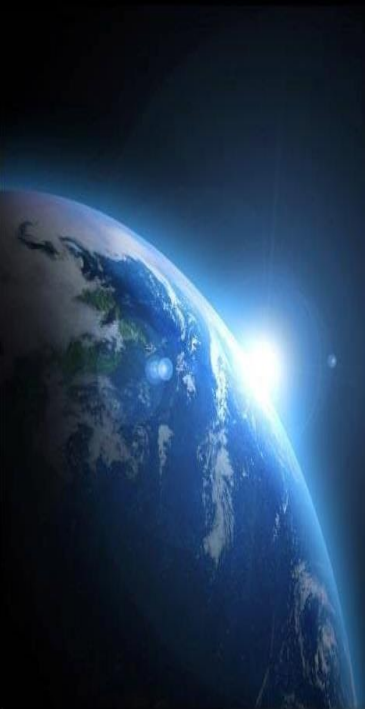
# Legislative and regulatory environment

- Directive 2016/1148 of 6 July 2016 to ensure a high level of security of networks and information systems: this directive will make it compulsory (as of May 2018) for critical operators (with the operator and many of its major Customers being classed as such to:

- Put in place appropriate measures to prevent incidents that compromise the security of networks and information systems;
- Adopt necessary and proportionate technical and organisational measures to manage risks to the security of networks and information systems;
- Provide prompt notification of incidents that have a significant impact on the continuity of the essential services they provide.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



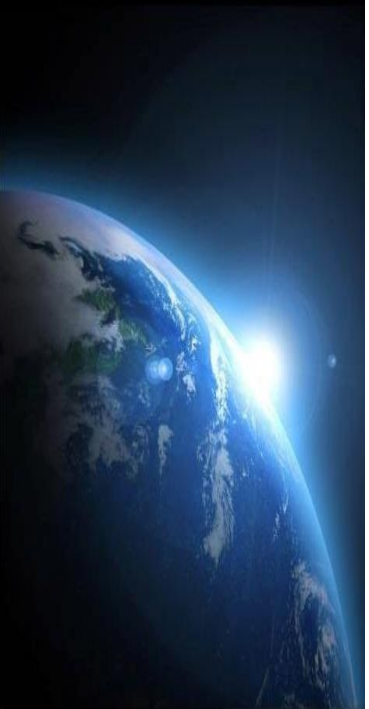
# Legislative and regulatory environment

**Germany**

- Berlin starts National Cyber Defense Initiative: On 16 June 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Abschirmdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organization founded on 23 February 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



# Legislative and regulatory environment

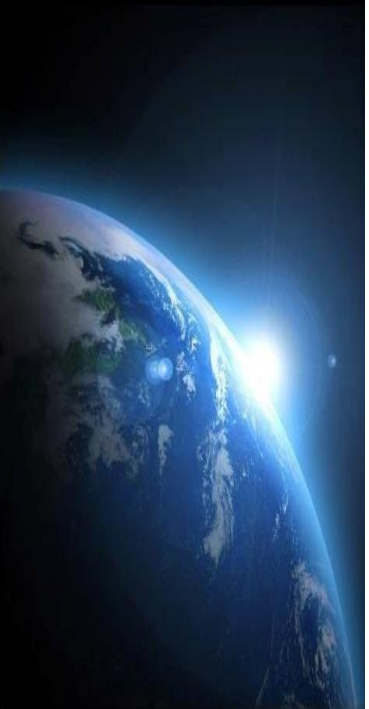
**United States**

**Legislation**

- The 1986 18 U.S.C. § 1030, more commonly known as the Computer Fraud and Abuse Act is the key legislation. It prohibits unauthorized access or damage of "protected computers" as defined in 18 U.S.C. § 1030(e)(2).
- Although various other measures have been proposed, such as the "Cybersecurity Act of 2010 – S. 773" in 2009, the "International Cybercrime Reporting and Cooperation Act – H.R.4962“ and "Protecting Cyberspace as a National Asset Act of 2010 – S.3480“ in 2010 – none of these has succeeded.
- Executive order 13636 *Improving Critical Infrastructure Cybersecurity* was signed 12 February 2013.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



# Contractual guidelines

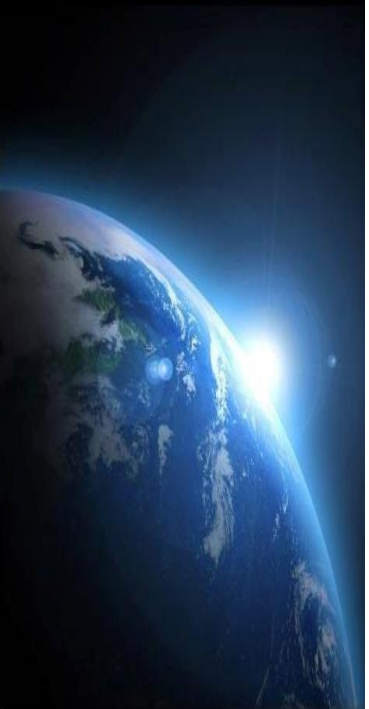
- **Guidelines as part of a Customer Agreement**

☑ Compliance with technical requirements: Ensure that customer requirements for cybersecurity are indeed met by the operator through delivery of a solution that reflects current knowledge existing on the date of signature of the agreement. Any changes will be taken care of by the customer by means of an amendment.

☑ Limiting the level of commitment: Limit the operator's commitment to a best efforts obligation and be able to demonstrate our diligence, retain the evidence demonstrating that we have fulfilled our duty to inform. (e.g., successive offers, customer alert on the capabilities of the solution and its limitations, etc.).

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



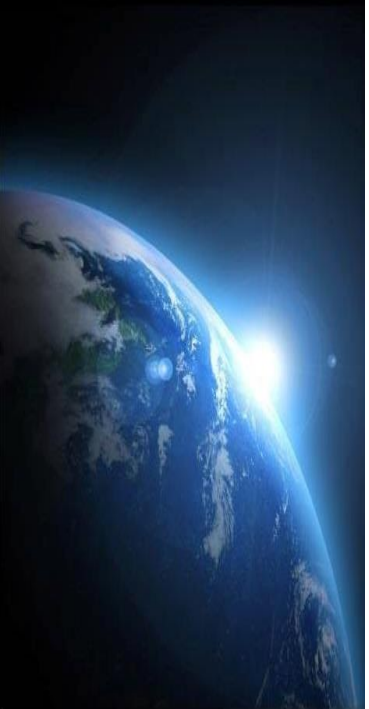
# Contractual guidelines

☑ Limited liability: Include in the upper limit of liability the effects of any security breaches and/or non-compliance with cybersecurity developments reflecting current knowledge. : If the customer so requests, it is possible for them to carry out audits or request them to be carried out at the operator (to the extent possible, these audits should not be carried out by the customer directly but rather by an independent third party chosen by the operator, and the frequency of such audits should be reasonable).

☑ Audits: If the customer so requests, it is possible for them to carry out audits or request them to be carried out at the operator (to the extent possible, these audits should not be carried out by the customer directly but rather by an independent third party chosen by the operator, and the frequency of such audits should be reasonable).

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



# Contractual guidelines

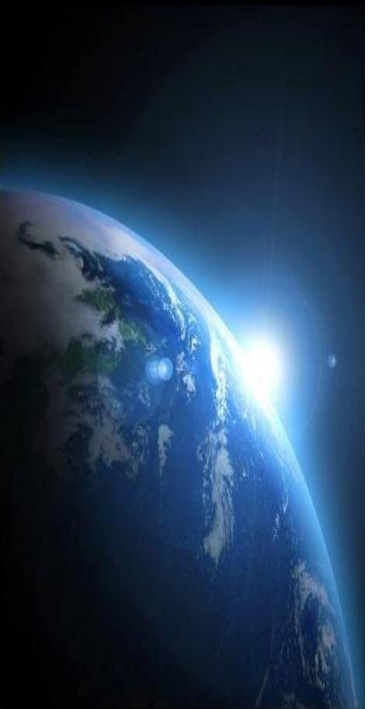
- **Guidelines as part of a purchase agreement**

☑ Compliance with technical requirements:

- Stipulate a clause relating to the obligation of the provider to put in place a certain number of security measures in order to limit the risks of unauthorised access and generally speaking the effects of a security breach.
- Reinforce the level of commitment of the provider by entering into performance obligations (i.e., in case of breach, the provider will be presumed liable unless it can show that the failure was due to an occurrence of force majeure or a wrongful act on the part of the operator).
- Identify the obligations in terms of essential obligations security in order to ascertain the scope of these obligations.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



# Contractual guidelines

- **Guidelines as part of a purchase agreement**

☑ Liability:

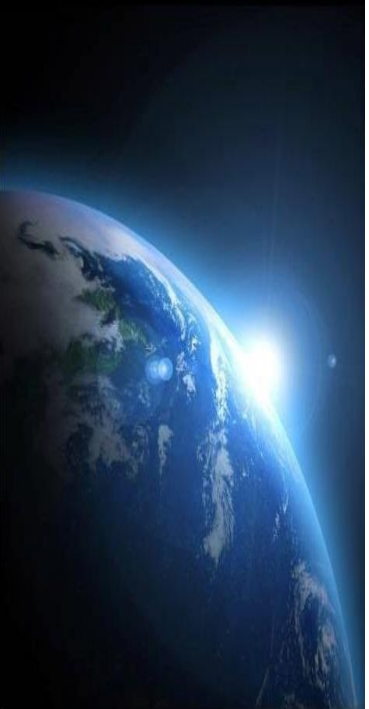
- Negotiate to have no upper limit of liability in the event of a security breach, loss of data and/or non-compliance with cybersecurity provisions.
- Contractually identify as direct damage the data recovery costs

☑ Audits:

- Have the right to carry out audits on providers; the audit clause should also specify the rules and penalties applicable to the audit procedure.
- Require the service provider to carry out audits on its own service providers.
- Have the right to obtain the audit reports produced by the service provider from its own processors.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

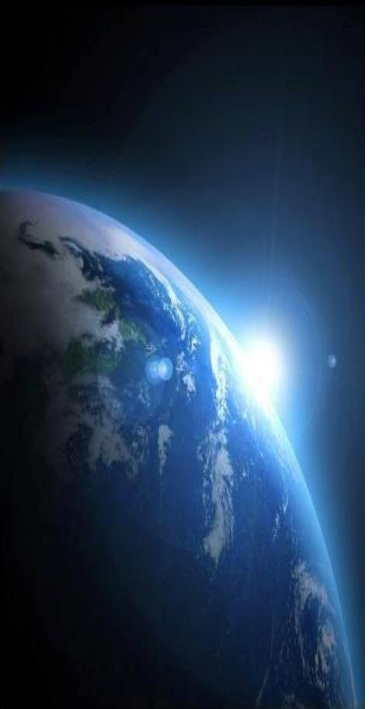


# Other recommendations to maximise legal security

- ☑ Structure: Set up a multidisciplinary team in charge of defining the cybersecurity strategy.
- ☑ Governance: Establish a specific crisis management policy in the event of a security breach and cyberattack. Update policies for the operator on security and business continuity policy in the event of a cyberattack.
- ☑ Training: Create guidelines that all employees can refer to and put in place training to ensure that they all know what to do when needed.
- ☑ Relations with authorities: Play an influential role in Country's cyberstrategy, particularly in the context of the national enactment of European laws and the implementation of national regulations.

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

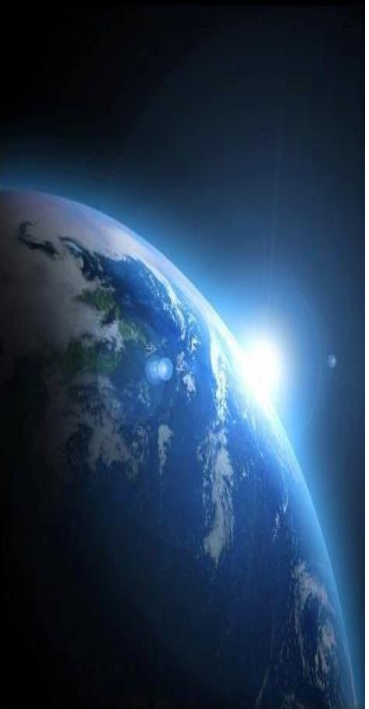


# Standard clauses with a client

| Recommendations | Proposed clauses |
|---|---|
| The operator shall ensure that the requirements made by its clients with regard to cyber-security may actually be implemented by same operator and that they are approved as state-of-the-art when the contract is signed: any changes must be borne by the client, by amendment to the Contract. | Integrate in the clause related to changes / amendments the fact that the impacts of standards and regulations' evolutions shall be borne by the Client. |
| When the operator provides a security solution, minimising its level of commitment (ex: obligations of means). If it's difficult with respect to the purpose of the contract in particular: (i) absence of pre-qualification at the commitment level and (ii) alert the client to the capacities and limits of a solution, in order to ensure perfect transparency. | The operator undertakes to provide the Client with the services stipulated in the Contract, in compliance with the specifications listed in Annex [●]. The Client acknowledges that it is aware of these specifications and with the restrictions associated with use [of the solution/services provided]. |

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

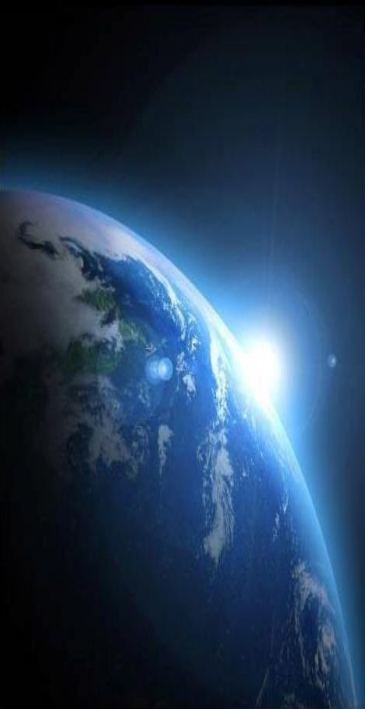


# Standard clauses with a client

| Recommendations | Proposed clauses |
|---|---|
| Negotiate the limitation of the liability cap in the event of a security breach and/or non-compliance with legal provisions concerning cyber-security. | It is understood that the limit to liability stipulated in clause [●] will apply in the event of a security breach and/or non-compliance with legal provisions concerning cyber-security.<br><br>Neither of the Parties shall be liable in the event of failure or lack of hardware, networks and/or security services provided by: (i) third parties (such as, without this list being exhaustive: software publishers, providers of security services, suppliers of equipment); or (ii) the other Party. |

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

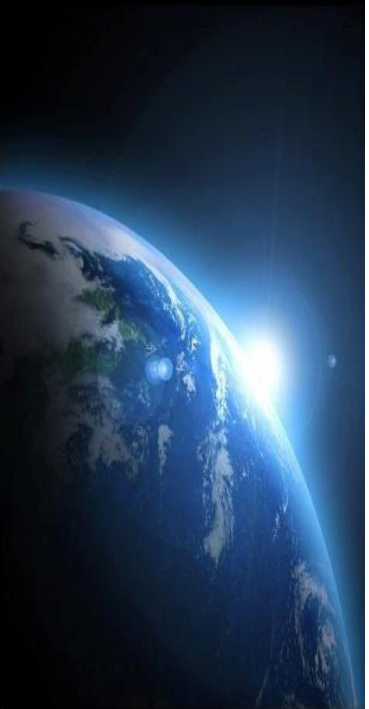


# Standard clauses with a client

| Recommendations | Proposed clauses |
|---|---|
| Accept that the client may perform audits on the operator but try to ensure, as far as possible, that these audits are not performed by the client directly but by an independent third party chosen by the operator.<br><br>Ensure that the frequency of the audits is reasonable to avoid jeopardising the operator security systems. | The audits may only be performed during normal business hours and no more than once a year, at the Client's expense. The review may only concern the twelve months of activity immediately preceding the audit. The Client and its auditors may not audit: (i) data or information relating to other clients and prospective clients of the operator; (ii) any the operator proprietary internal data (including information on cost structure as well as any financial and accounting data); or (iii) any other "Confidential Information" belonging to the operator which does not directly or strictly concern the purposes of the audit. The Client shall notify the operator in writing, within at least fifteen (15) days' notice, of its decision to proceed with the audit, specifying its scope and methods. Audits may only be performed by an independent third party chosen by the operator. The Client's auditors and other representatives will perform and comply with the confidentiality and non-disclosure agreements. They will comply with the security and confidentiality measures required by the operator for its audits. |

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

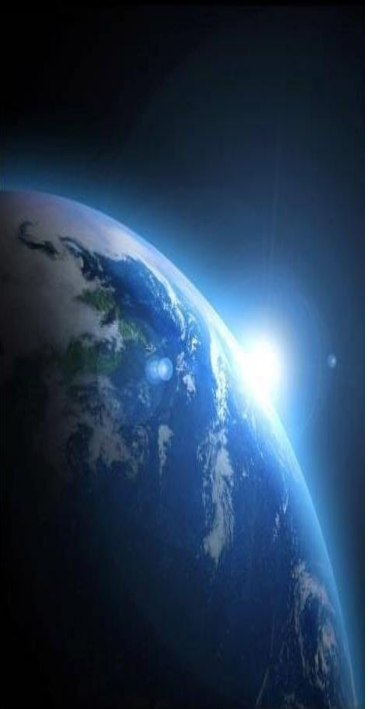


# Standard clauses with a service provider

| Recommendations | Proposed clauses |
|---|---|
| Provide for a clause relating to service provider's duty to introduce security measures limiting the risk of unauthorised access and the general impact of cyber-security breaches. | The Service Provider acknowledges that security (to be defined in the contract) is of fundamental concern for the operator and that the Service Provider's compliance with the operator' security regulations, rules and procedures is an essential and determining condition of the operator' agreement to enter into this Contract.<br>The Service Provider guarantees compliance with the security obligations described in [●]. The Service Provider guarantees compliance with these provisions by its staff and any sub-contractors.<br>If a breach or the risk of a breach is discovered by, or reported to, the Service Provider or its sub-contractors, the Service Provider must immediately inform the operator when the potential or actual breach is discovered, and in any event within twenty-four (24) hours of the event. |

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

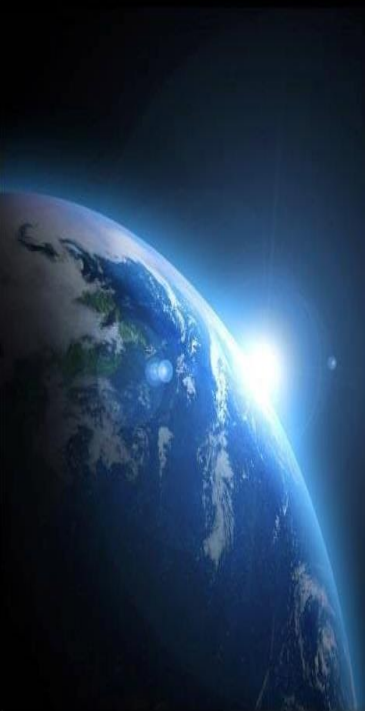


# Standard clauses with a service provider

| Recommendations | Proposed clauses |
|---|---|
| | The Service Provider must take all the measures it deems necessary and appropriate to ensure that none of its staff, agents or service providers has access to the operator' documents, files, information, data, databases and IT systems (hereinafter the "**Information Resources**") without express authorisation. In the event of access to the Information Resources, the Service Provider undertakes to respect the procedures of the operator, particularly regarding the access, use and security of the Information Resources.<br>The Service Provider undertakes to not communicate with third parties or the authorities regarding a potential or actual security breach without the prior written consent of the operator. |
| Describe in annex the security measures expected by the operator | On a case by case basis. |

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

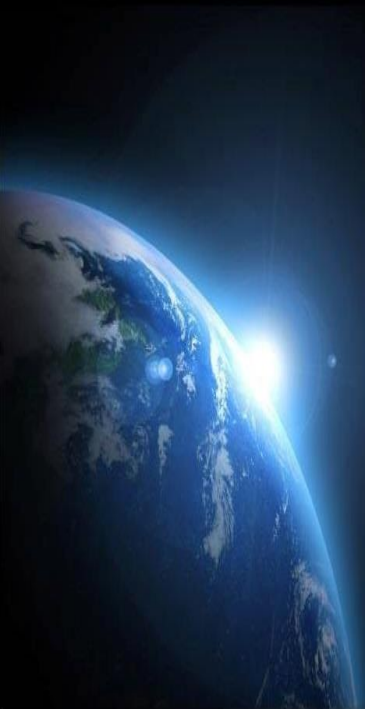


# Standard clauses with a service provider

| Recommendations | Proposed clauses |
|---|---|
| Strengthen the Service Provider's level of commitment by pre-qualifying its obligations in respect of security as an obligation of result (i.e. in the event of failure, the Service Provider will be presumed liable, unless it can prove that the failure resulted from force majeure or the fault of the operator). | The Service Provider, in its capacity as a professional provider of [●] services, undertakes to provide the operator with the services defined in the Contract and, in particular, the security services described in Annex [●], as part of its obligation of result, notwithstanding any stipulation to the contrary provided for in the Contract [...]. |
| Qualify the security obligations as essential obligations for ensuring the full effectiveness of these comitments | It is understood that the Service Provider's compliance with its security obligations as described in the Contract and in Annex [●] constitute essential and determining obligations of the Contract, without which the operator would not have entered into this Contract. |

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

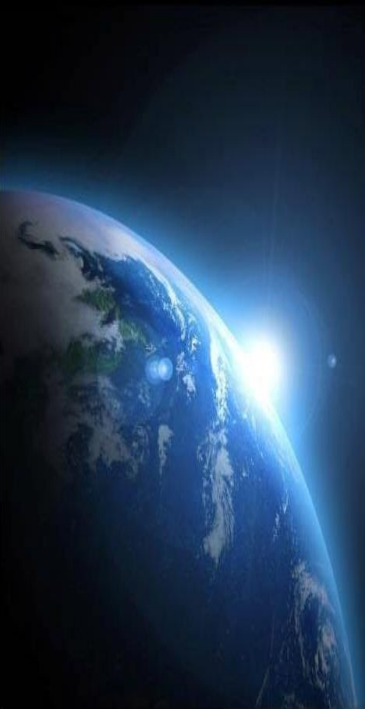


# Standard clauses with a service provider

| Recommendations | Proposed clauses |
|---|---|
| Negotiate the absence of a limit to liability in the event of a security breach, data loss and/or non-compliance with legal provisions relating to cyber-security. | The Service Provider may not claim limited liability in the event of:<br>• security breach<br>• data loss<br>• non-compliance with legal provisions relating to cyber-security.<br>• non-compliance with the security obligations set out in the Contract and in Annex [●],<br>• […]. |
| Pre-qualify as direct damage the cost of recovering data. | The Parties may only be held liable for direct damage it being understood that damage resulting from [...], from data loss and recovery, from the loss of turnover and market as well as damage to the reputation of the operator, resulting from the Service Provider's failure to comply with security measures are considered to be direct damages for which compensation may be provided under the Contract. |

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

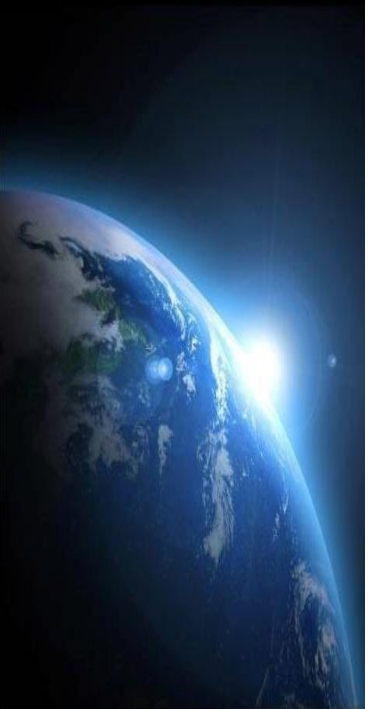


# Standard clauses with a service provider

| Recommendations | Proposed clauses |
|---|---|
| Have the right to audit the service providers.<br><br>The audit clause should also specify the rules and penalties applicable to the audit procedure | The Parties agree that the operator has the right to monitor and to audit, in the manner and on the terms for implementation specified below.<br><br>The operator may conduct audits on the Service Provider's premises, at the operator's expense, not more than [●] time(s) per year except in the event of: (i) serious non-performance (examples: non-compliance with security obligations; attempts to interfere with the operator' data) of the Service Provider's obligations; or (ii) a follow-up audit conducted after a failure by the Service Provider as established by the audit report; or (iii) [...]:<br><br>• on condition that the Service Provider is notified at least [●] days in advance, or without warning in the event of a security breach or serious non-performance by the Service Provider; and<br><br>• either performed by itself (for example, using its own internal audit teams), or by using the services of an well-known audit firm; and |

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

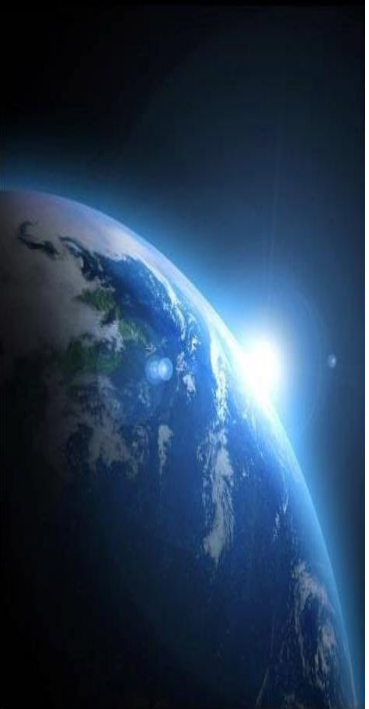


# Standard clauses with a service provider

| Recommendations | Proposed clauses |
|---|---|
| | • in order to: (i) assess the progress and quality of the Services provided; (ii) verify their compliance with the rules and procedures defined in this Contract; (iii) verify compliance with the Service Provider's obligations regarding security and the protection of personal data; (iv) verify the Service Provider's compliance with the applicable laws; or (v) for any other purpose, provided that the audit had no other purpose than ensuring the Service Provider's fulfilment of it obligations under the Contract.<br><br>In any event, the appointed auditor must sign a confidentiality agreement. |

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA



# Standard clauses with a service provider

| Recommendations | Proposed clauses |
|---|---|
| Provide for the ability to require the service provider to perform audits on its own service providers. | The Parties agree that the operator may request that the Service Provider perform audits of the Service Provider's sub-contractors, particularly with regard to security measures. |
| Provide for the ability to obtain the audit reports produced by the Service Provider when auditing its own sub-contractors. | In any event, the Service Provider undertakes to provide the operator with the audit reports concerning the audits performed by the Service Provider on its sub-contractors (particularly with regard to security) once they have been issued, or in any event within [●] days following their issue. |