Cigref

SUCCEED WITH DIGITAL

Cigref

Trusted cloud

REFERENCE DOCUMENT

v.2 *– October 2022*

Trusted cloud
REFERENCE DOCUMENT

INTRODUCTION

Cigref's "**trusted cloud" referential** expresses the **generic trust needs** of Cigref members **as users of cloud services**. It summarizes Cigref's work carried out since 2019 by the "trusted cloud" working group, led by Vincent Niebel, CIO of the EDF Group.

This version, known as V2, takes into account the comments received during the call for comments on version V1 from Gaia-X European hubs and European user associations. This amended version includes **a new and fourth axis aimed at characterizing the control of the environmental footprint of cloud services**, in addition to the axes of security, control of dependencies on suppliers and immunity to non-European laws.

Before specifying the ambitions of this referential and the new features of this version, let's review the objectives of the Trusted Cloud Referential.

Why a trusted cloud referential for digital service users?

Cloud computing offers significant benefits and is now the must-have in terms of cost, flexibility, efficiency, optimization, security and scalability for its public and private sector customers. Cloud computing is now the technology sector, both in terms of infrastructure and software products, that leads all others.

Businesses are looking **for trust in the cloud in order to greatly reduce their exposure to geopolitical and legal risks, as well as to interference and intelligence activities of economic interest**. Indeed, for companies and public administrations, "to control your dependencies is to control your destiny". And they express their needs, particularly in the digital field, in terms of controlling their dependencies, which are based on the main economic, geopolitical and strategic concerns.

1. Enable businesses and public administrations to preserve their autonomy of assessment, decision and action, particularly with regard to their cloud service providers. For users, it is a question of controlling their dependence on the strategy of locking in cloud providers who are in a hegemonic position on the European cloud market. In this respect, the provisions of the European Digital Markets Act, relating to gatekeepers, and those under discussion in the Data Act, are welcomed by users.
2. Anticipate the geostrategic dependence of our economy on non-European digital solutions. What happens in the event of blackmail on access to the resources of foreign cloud providers, targeting a company, a sector of activity, a State or the whole of the EU? The threat of a foreign power turning off the digital energy tap should be considered as a strategic risk.
3. Protect the sensitive personal and non-personal information assets of companies and public administrations from legal access by non-European legislation with extraterritorial reach.

Ambitions for the trusted cloud

The aim of Cigref's collective intelligence work is to **characterise trust** as expressed by Cigref's members in terms of cloud solutions and services for **the protection of their sensitive data and associated processing**. This trusted cloud referential translates this need into **functional and objective requirements.**

This version 2 of the referential therefore sets out the requirements of the trust around 4 axes, the axis of **security** / cybersecurity, the axis of **control of dependence on suppliers**, the axis of **immunity to**

non-European laws, and the new axis aiming to characterise the **control of the environmental footprint of cloud services**. This new requirement calls for transparency on the part of cloud providers. Most of them present the efforts they can make in this area in a formalism that is hardly compatible with an objective understanding of their real effects on their customers and their uses.

This version 2 of Cigref's "trusted cloud" guidelines will, of course, evolve in the coming months to take into account technological, economic and regulatory developments that may have an impact on the characteristics of the cloud market and on the protection of sensitive data of Cigref members.

Some clarifications

For sensitive non-personal data, it is particularly important to guard against the risks posed by foreign laws with extraterritorial scope for data collection, such as Section 702 of the US Foreign Intelligence & Surveillance Act (Executive Order 12 333), which was highlighted in the European Union Court of Justice's judgment of 16 July 2020 invalidating the *Privacy Shield* in the context of the "*Shremes* II" case, or the Chinese National Intelligence Law of 28 June 2017, and in particular Articles 7 and 10 .

If Europe were to continue on its current trajectory and given the exponential growth of the public cloud market, within ten years or so, 90% of this market could be pre-empted by three American players who would have the possibility of constraining or even locking in their solutions and services to most of the most essential processes of all European companies and public administrations. And, to date, the competition to these players seems likely to come mainly from China.

Cigref is not in any way involved in a strategy to drive American suppliers out of the European market. Europe's digital autarky is a chimera that can often mask protectionist aims. However, if the European digital market is to remain open, it must not be open to just any wind. This is why Cigref calls for the particular and short-term interests of companies and public administrations to be articulated, particularly through regulation. In this way, the latter will be able to benefit from the best solutions for their competitiveness, while taking into account the medium- and long-term risks that the loss of autonomy of the European continent in terms of digital technologies poses to the general interest and to the European economy.

GLOSSARY

1.1. ACRONYMS

Acronym	Definition
API	Application Programming Interface
CSA	Contract Service Agreement
CSC	Cloud Service Customer
CSP	Cloud Service Provider
Export	Data export from the cloud to the CSC
IaaS	Infrastructure as a Service
Import	Data import from the CSC to the cloud
NDA	Non-Disclosure Agreement
Portability	The right for any consumer to recover all of their data and to transfer it to another operator while continuing to use the service
Reversibility	The right of any consumer to recover all of their data and to transfer it to another operator on termination of the contract
SaaS	Software as a Service
SLA	Service Level Agreement
SLO	Service Level Objective
SQO	Service Qualitative Objective

1.2. LEVELS OF TRUST

Safe Cloud - The proposed rules are key to ensuring a foundation of trust.

Trusted Cloud - The proposed rules reinforce the "Safe" level for more specific trust needs.

REVISION TABLE

VERSION HISTORY			
No.	Date of update	Author	Description of the updates
V.01	25/05/2021	Magellan Consulting	First version
V.02	26/05/2021	Baptiste Chauveau	Layout and table of contents
V.2	24/10/2022	Cigref	Transparency with respect to applicable legal regimes, Immunity to extraterritorial laws Environmental impacts of digital technology (hardware and software)

1 GENERAL CONTRACTUAL REQUIREMENTS

The following requirements are considered generic and to be included in all contracts.

1.1. GENERAL CONTRACT CLAUSES

Requirements to ensure a "Safe Cloud" level of trust

GEN-1-SAFE-1. The contract or any binding legal act between the CSP and the CSC shall be subject to the competent jurisdiction of an EU Member State.

GEN-1-SAFE-2. The CSA must be documented (including in electronic form) and legally binding between the infrastructure CSP and the CSC.

GEN-1-SAFE-3. The CSA may take any form, including, but not limited to: a) a single contract; b) a set of documents such as a basic service agreement with relevant annexes (data processing agreements, SLAs, terms of service, security policies, etc.); or c) the standard online terms and conditions.

GEN-1-SAFE-4. The CSP must continuously identify the current legal, regulatory and contractual requirements applicable to the service. It must document and implement procedures to comply with the applicable legal, regulatory and contractual requirements for the service, as well as specific security needs. These measures are available to the CSC on request.

Requirements to ensure a "Trusted Cloud" level of trust

GEN-1-TRUSTED-5. The CSP must provide the CSC with a clear description of policies on access and porting of data in the event of CSP bankruptcy, the occurrence of ransomware problems or the acquisition of the CSP by another entity.

2 SECURITY REQUIREMENTS

2.1. INFORMATION SECURITY POLICY AND RISK MANAGEMENT

Requirements to ensure a "Safe Cloud" level of trust

SEC-1-SAFE-1. A general information security policy must be written, broken down into policies and procedures for security requirements and for meeting the requirements of the CSP. This policy must identify the CSP's commitments to comply with the relevant legislation and regulations. The CSC remains responsible for compliance with the legal and regulatory constraints applicable to the data it entrusts to the CSP.

SEC-1-SAFE-2. The policy must:

- Cover all topics in the 14 security chapters of this document,
- Be formally approved by the CSP management,
- Be reviewed annually and whenever there is a major change that may have an impact on the service.

SEC-1-SAFE-3. It must be ensured that the information security risks are properly identified, assessed and handled, and that the residual risk is formally accepted by the CSP management.

SEC-1-SAFE-4. The risk analysis must be reviewed by the CSP annually and whenever there is a major change that may have an impact on the service.

SEC-1-SAFE-5. The CSP must carry out its risk assessment using a documented method that guarantees the reproducibility and comparability of the approach.

SEC-1-SAFE-6. The CSP must take into account in the risk assessment:

- Management of information from CSCs with different security needs;
- The risks impacting the rights and freedoms of data subjects in the event of unauthorised access, unwanted modification and disappearance of personal data,
- The risks of failure of the partitioning mechanisms of the technical infrastructure resources (memory, calculation, storage, network) shared between the CSCs,
- The risks related to incomplete or unsecured deletion of data stored on memory or storage spaces shared between CSCs, in particular when reallocating memory and storage spaces,
- The risks associated with exposing administrative interfaces on a public network.

SEC-1-SAFE-7. Where there are specific legal, regulatory or sector-based requirements relating to the types of information that the CSC may entrust to the CSP, the latter must take them into account in its risk assessment by ensuring that it complies with all the requirements of this reference document on the one hand, and that it does not lower the level of security established by compliance with the requirements of this reference document on the other.

2.2. INFORMATION SECURITY ORGANISATION

Requirements to ensure a "Safe Cloud" level of trust

SEC-2-SAFE-1. It is essential to plan, implement, maintain and continuously improve the information security framework within the organisation. This organisation includes the appointment of an information systems security officer and a physical security officer (if relevant).

SEC-2-SAFE-2. The CSP must identify the risks associated with the accumulation of responsibilities or tasks, take them into account in the risk assessment and implement measures to reduce these risks.

SEC-2-SAFE-3. The CSP must document a risk assessment prior to any project that may have an impact on the service, regardless of the nature of the project. If a project affects or is likely to affect the service security level, the CSP must notify the CSC and inform them in writing of the potential impacts, the measures put in place to reduce these impacts and the residual risks affecting them.

Requirements to ensure a "Trusted Cloud" level of trust

SEC-2-TRUSTED-4. The CSP is advised to establish appropriate relations with the competent authorities for the security of information and personal data and, where appropriate, with the sectoral authorities, depending on the nature of the information entrusted by the CSC to the CSP.

SEC-2-TRUSTED-5. The CSP is advised to maintain appropriate contacts with specialist groups or recognised sources, in particular in order to consider new threats and appropriate security measures to counter them.

2.3. HUMAN RESOURCES SECURITY

Requirements to ensure a "Safe Cloud" level of trust

SEC-3-SAFE-1. The CSP must document and implement a procedure for the verification of information concerning its personnel, in accordance with the applicable laws and regulations. These checks apply to everyone involved in the provision of the service and must be proportionate to the sensitivity of the contracting party's information entrusted to the CSP and the risks identified.

SEC-3-SAFE-2. The CSP must ensure that its employees understand their responsibilities, are aware of their responsibility for information security, and that the organisation's assets are protected in the event of a change of responsibility or termination of employment.

SEC-3-SAFE-3. The CSP must have a charter of ethics which is integrated into the internal rules and regulations, stipulating in particular that:

- Services are provided with loyalty, discretion, impartiality and respecting the confidentiality of the information processed,
- Personnel only use methods, tools and techniques validated by the CSP,
- Personnel undertake not to divulge to a third party any information, even anonymised and decontextualised, obtained or generated within the context of the service, unless formally authorised in writing by the CSC,

- Personnel undertake to report to the CSP any manifestly illegal content discovered during the service,
- Personnel undertake to comply with the national laws and regulations in force and with good practice in relation to their activities.

SEC-3-SAFE-4. The CSP must have all parties involved in the provision of the service sign the ethics charter.

SEC-3-SAFE-5. The CSP must, upon request from the CSC, make available to them the internal rules and the ethics charter.

SEC-3-SAFE-6. The CSP must raise awareness of information security and data protection risks among all those involved in the provision of the service. It must inform them of any updates to policies and procedures relevant to their missions. The CSP must document and implement an information security training plan tailored to the service and the personnel's tasks. The CSP's information systems security officer must formally validate the information security training plan.

SEC-3-SAFE-7. The CSP must document and implement a disciplinary process applicable to all persons involved in the provision of the service who have breached the security policy. The CSP must, upon request from the CSC, make available to them the sanctions incurred for breaches of the security policy.

SEC-3-SAFE-8. The CSP must define and assign roles and responsibilities for the termination, conclusion or modification of any contract with a person involved in the provision of the service.

2.4. ASSET MANAGEMENT

Requirements to ensure a "Safe Cloud" level of trust

SEC-4-SAFE-1. It is essential to identify the organisation's own assets and ensure an appropriate level of protection throughout their life cycle. This inventory must be kept up to date.

SEC-4-SAFE-2. The CSP must document and implement an asset return procedure to ensure that each person involved in providing the service returns all assets in their possession at the end of their employment or contract.

SEC-4-SAFE-3. The CSP must identify the different security needs for information relating to the service. Where the CSC may entrust the CSP with data subject to specific legal, regulatory or sector-based constraints, the CSP must identify the specific security requirements associated with these constraints.

SEC-4-SAFE-4. The CSP must document and implement a procedure for the management of removable media that is appropriate to the security needs of the data services with which they may be entrusted by the customers. Where removable media are used on the technical infrastructure or for administrative tasks, these media should be dedicated to a single purpose.

SEC-4-SAFE-5. The CSP is advised to document and implement a procedure for the marking and handling of all information involved in the delivery of the service, in accordance with its security needs.

2.5. ACCESS CONTROL AND IDENTITY MANAGEMENT

Requirements to ensure a "Safe Cloud" level of trust

SEC-5-SAFE-1. It is essential to limit access to information processing facilities and to the information itself.

SEC-5-SAFE-2. Unless explicitly stated, this chapter deals with access control and the identity management of users:

- For whom the CSP is responsible (its employees and possibly third parties involved in providing the service),
- For whom the CSC is responsible, but for whom the service provider implements the means of access control (in particular by providing the CSC with an interface for managing accounts and access rights).

Users for whom the contracting party implements the means of access control and identity management fall outside the scope of this reference document.

SEC-5-SAFE-3. The CSP must document and implement an access control policy based on the outcome of its risk assessment and the sharing of responsibilities. The CSP must review the access control policy annually and whenever there is a major change that may have an impact on the service.

SEC-5-SAFE-4. The CSP must document and implement a user registration and de-registration procedure based on an interface for managing accounts and access rights. This procedure must indicate which data must be deleted when a user leaves.

SEC-5-SAFE-5. The CSP must assign named accounts when registering users under its responsibility.

SEC-5-SAFE-6. The CSP must implement means to ensure that the de-registration of a user results in the deletion of all access to the service's IT resources and the deletion of the user's data in accordance with the registration and de-registration procedure.

SEC-5-SAFE-7. The CSP must document and implement a procedure to ensure the granting, modification and withdrawal of access rights to the service's IT resources.

SEC-5-SAFE-8. The CSP must provide the contracting party with the tools and means to differentiate the roles of the service users, for example based on their functional role.

SEC-5-SAFE-9. The CSP must maintain an up-to-date inventory of users for which it is responsible, who have administrator rights for the service's IT resources.

SEC-5-SAFE-10. The CSP must be able to provide, for a given resource implementing the service, a list of all users with access to it, whether they are the responsibility of the CSP or the CSC, and the access rights that have been assigned to them.

SEC-5-SAFE-11. The CSP must be able to provide for a given user, whether they are the responsibility of the CSP or the CSC, a list of all their access rights to the various elements of the service's IT system.

SEC-5-SAFE-12. The CSP must include in the access rights management procedure the actions to revoke or suspend the rights of any user.

SEC-5-SAFE-13. The CSP must review annually the access rights of users for which it is responsible.

SEC-5-SAFE-14. The CSP must provide the CSC with a tool to facilitate the review of access rights of users for which they are responsible.

SEC-5-SAFE-15. The CSP shall review quarterly the list of users for which it is responsible who may use the technical accounts.

SEC-5-SAFE-16. The CSP must formalise and implement procedures for managing user authentication. In accordance with the requirements of the "cryptology" chapter, these must include:

- Management of authentication means (issuing and resetting passwords, updating CRLs and importing root certificates when using certificates, etc.).
- Implementation of the means allowing multi-factor authentication to meet the different usage cases of the reference document.
- Systems that generate passwords or check their strength, where password authentication is used.

SEC-5-SAFE-17. All authentication mechanisms must allow for the blocking of an account after a limited number of unsuccessful attempts.

SEC-5-SAFE-18. In the context of an SaaS service, the CSP must provide the CSC with multi-factor authentication means for end-user access.

SEC-5-SAFE-19. Where non-named technical accounts are required on the SaaS service, the CSP must provide the CSC with the means to require users to log in using their named account before being able to access these technical accounts.

SEC-5-SAFE-20. Administration accounts under the responsibility of the CSP must be managed using separate tools and directories from those used for the management of user accounts under the responsibility of the CSC.

SEC-5-SAFE-21. The administration interfaces made available to the CSC must be different to the administration interfaces used by the CSP. The administration interfaces made available to the CSC must not allow any connection with administrator accounts under the responsibility of the CSP.

SEC-5-SAFE-22. The administration interfaces used by the CSP must not be accessible from a public network and must not therefore allow any connection of users under the responsibility of the CSC. If administration interfaces are made available to the CSC with access via a public network, the administration flows must be authenticated and encrypted with means in accordance with the requirements.

SEC-5-SAFE-23. The CSP must implement a two-factor authentication system for access to:

- Administration interfaces used by the CSP,
- Administration interfaces dedicated to CSCs.

SEC-5-SAFE-24. In the context of an SaaS service, the administration interfaces made available to the CSCs must be distinguished from the interfaces for end-user access.

SEC-5-SAFE-25. If an administration interface is accessible from a public network, the authentication process must take place before any interaction between the user and the interface in question.

SEC-5-SAFE-26. When the CSP uses an IaaS service as the basis for another type of service (PaaS or SaaS), the resources allocated to the CSP's use must not under any circumstances be accessible via the public interface made available to other CSCs of the IaaS service. When the CSP uses a PaaS service as the basis for another type of service (typically SaaS), the resources allocated to the CSP's use must not under any circumstances be accessible via the public interface made available to other CSCs of the PaaS service.

SEC-5-SAFE-27. The CSP must implement appropriate partitioning measures between its CSCs.

SEC-5-SAFE-28. The CSP must implement appropriate partitioning measures between the service's IT system and its other IT systems (office automation, in-business computing, building technical management, physical access control, etc.).

SEC-5-SAFE-29. The CSP must design, develop, configure and deploy the service's IT system, ensuring partitioning at least between the technical infrastructure on the one hand and the equipment necessary for the administration of the services and the resources it hosts on the other.

Requirements to ensure a "Trusted Cloud" level of trust

SEC-5-TRUSTED-30. The CSP must specify the security controls (e.g. access controls) used when importing data.

2.6. CRYPTOLOGY

Requirements to ensure a "Safe Cloud" level of trust

SEC-6-SAFE-1. It is necessary to ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.

SEC-6-SAFE-2. The CSP must define and implement an encryption mechanism that prevents the recovery of CSC data in the event of reallocation of a resource or recovery of the physical media. In the case of an IaaS service, this objective can be achieved, for example:

- By disk or file system encryption, where the file mode access protocol ensures that only empty blocks can be allocated (e.g. NAS-type storage in which a physical block is only effectively allocated at the time of writing),
- By volume-based encryption in the case of block access (e.g. SAN or local storage), with at least one key per CSC,
- In the case of a PaaS or SaaS service, this can be achieved by using application encryption within the CSP scope, with at least one key per CSC.

SEC-6-SAFE-3. The CSP must offer a catalogue of data encryption methods enabling the CSC to comply with the rules of its relevant authorities.

SEC-6-SAFE-4. The CSP must implement encryption of data on removable media and backup media that need to be taken outside of the physical security perimeter of the service's IT system, depending on the data security needs.

SEC-6-SAFE-5. When the CSP implements a network flow encryption mechanism, this mechanism must comply with the recommendations of the relevant authorities (French National Agency for the Security of Information Systems (ANSSI), German Federal Office for Information Security (BSI), etc.).

SEC-6-SAFE-6. The CSP must only store the fingerprint of user passwords and technical accounts. The fingerprints must be generated with a hash function associated with the use of a cryptographic salt respecting the recommendations of the relevant authorities (ANSSI, BSI, etc.).

SEC-6-SAFE-7. When the CSP implements an electronic signature mechanism, this mechanism must comply with the recommendations of the relevant authorities (ANSSI, BSI, etc.).

SEC-6-SAFE-8. The CSP must use cryptographic keys that comply with the recommendations of the relevant authorities (ANSSI, BSI, etc.).

SEC-6-SAFE-9. The CSP must protect access to the cryptographic keys and other secrets used for data encryption by suitable means: security container (software or hardware) or separate media. The CSP must protect access to cryptographic keys and other secrets used for administrative tasks with a suitable security container, software or hardware.

2.7. PHYSICAL & ENVIRONMENTAL SECURITY

Requirements to ensure a "Safe Cloud" level of trust

SEC-7-SAFE-1. Means must be implemented to prevent unauthorised physical access and to protect against theft, damage, loss and failure of operations.

SEC-7-SAFE-2. The CSP must document and implement security scopes, including the marking of areas and the various means of limiting and controlling access. The CSP must distinguish between public areas, private areas and sensitive areas. Public areas are accessible to all within the boundaries of the CSP property. The CSP must not host any resources dedicated to the service or allowing access to components of the service in the public areas. Private areas may host the service development platforms and facilities, the administration, operation and supervision stations and the premises from which the CSP operates. Sensitive areas are reserved for hosting the service's production IT system, excluding administration, operation and supervision stations.

SEC-7-SAFE-3. The CSP must protect private areas from unauthorised access. To do so, it must implement physical access control based on at least one personal factor: knowledge of a secret, possession of an object or biometrics. The CSP must define and document exceptional physical access measures for emergency situations. The CSP must post a warning at the entrance to the private areas regarding the restrictions and conditions of access to these areas. The CSP must define and document the time slots and conditions of access to private areas based on the profiles of the parties involved. The CSP must document and implement the means to ensure that visitors are systematically accompanied by the CSP when accessing and remaining in the private area. The CSP must keep a record of the identity of visitors in accordance with the laws and regulations in force. The CSP must

document and implement mechanisms for monitoring and detecting unauthorised access to private areas.

SEC-7-SAFE-4. In the context of physical access control, the CSP must comply with the standards published by the relevant authorities (ANSSI, BSI, etc.).

SEC-7-SAFE-5. The CSP must protect sensitive areas from unauthorised access. To do so, it must implement physical access control based on at least two personal factors: knowledge of a secret, possession of an object or biometrics. The CSP must define and document exceptional physical access measures for emergency situations. The CSP must post a warning at the entrance to the sensitive areas regarding the restrictions and conditions of access to these areas. The CSP must define and document the time slots and conditions of access to sensitive areas based on the profiles of the parties involved. The CSP must document and implement the means to ensure that visitors are systematically accompanied by the CSP when accessing and remaining in the sensitive area. The CSP must keep a record of the identity of visitors in accordance with the laws and regulations in force. The CSP must document and implement mechanisms for monitoring and detecting unauthorised access to sensitive areas. The CSP must implement logging of physical access to sensitive areas. It must review these logs at least once a month. The CSP must implement means to ensure that no direct access exists between a public area and a sensitive area.

SEC-7-SAFE-6. The CSP must document and implement the means to minimise the risks inherent in physical (fire, water damage, etc.) and natural (climate risks, floods, earthquakes, etc.) disasters. The CSP must document and implement measures to limit the risk of fires starting or spreading, as well as the risks of water damage. The CSP must document and implement measures to prevent and limit the consequences of a power failure and to enable the service to be resumed in accordance with the service availability requirements defined in the service agreement. The CSP must document and implement the means to maintain appropriate temperature and humidity conditions for the equipment. In addition, it must implement measures to prevent air conditioning failures and limit their consequences. The CSP must document and implement regular controls and tests of detection and physical protection equipment.

SEC-7-SAFE-7. The CSP must integrate the physical security elements into the security policy and risk assessment in accordance with the level of security required by the category of the area. The CSP must document and implement procedures for working in private and sensitive areas. It must communicate these procedures to the parties involved.

SEC-7-SAFE-8. Delivery and loading areas and other points where unauthorised persons may enter the premises unaccompanied are considered public areas. The CSP must isolate the access points from these areas to private and sensitive areas, so as to prevent unauthorised access, or alternatively implement compensatory measures to ensure the same level of security.

SEC-7-SAFE-9. The CSP must document and implement measures to protect electrical and telecommunication wires from physical damage and possible interception. The CSP must produce a wiring plan and keep it updated.

SEC-7-SAFE-10. The CSP must document and implement measures to ensure that the conditions for installation, maintenance and servicing of the service's IT equipment hosted in private and sensitive areas are compatible with the service confidentiality and availability requirements as defined in the service agreement. The CSP must take out maintenance contracts to ensure that security updates

are available for the software installed on the service's IT equipment. The CSP must ensure that media can only be returned to a third party if the CSC data is stored on it encrypted in accordance with the "Cryptology" chapter or has been previously destroyed using a secure erasure mechanism by rewriting random patterns. The CSP must document and implement measures to ensure that the conditions for installation, maintenance and servicing of ancillary technical equipment (power supply, air conditioning, fire, etc.) are compatible with the service availability requirements defined in the service agreement.

SEC-7-SAFE-11. The CSP must document and implement a procedure for the off-site transfer of CSC data, equipment and software. This procedure must require written authorisation from the CSC management. In all cases, the CSP must implement the means to ensure that the level of protection in terms of confidentiality and integrity of assets during transport is equivalent to that on site.

SEC-7-SAFE-12. The CSP must document and implement means to securely erase any data media made available to the CSC by rewriting random patterns. If the storage space is encrypted with the mechanisms specified in the "cryptography" chapter, erasure can be achieved by securely erasing the encryption key.

SEC-7-SAFE-13. The CSP must document and implement a procedure for protecting equipment awaiting use.

2.8. OPERATIONAL SECURITY

Requirements to ensure a "Safe Cloud" level of trust

SEC-8-SAFE-1. It is necessary to ensure proper and regular operation, including appropriate measures for capacity planning and monitoring, malware protection, event recording and monitoring, and the management of vulnerabilities, malfunctions and failures.

SEC-8-SAFE-2. The CSP must provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers.

SEC-8-SAFE-3. The CSP must document operating procedures, keep them up to date and make them available to the relevant personnel.

SEC-8-SAFE-4. The CSP must document and implement a procedure for managing changes to information processing systems and facilities. The CSP must document and implement a procedure enabling the following information to be communicated as soon as possible to all its contracting parties in the event of operations carried out by the service provider which may have an impact on the security or availability of the service:

- The scheduled date and time of the start and end of operations,
- The nature of the operations,
- The impacts on the security or availability of the service,
- The contact person within the CSP.

SEC-8-SAFE-5. In the context of a PaaS service, the CSP must inform the CSC as soon as possible of any future changes to software elements for which it is responsible if full compatibility cannot be ensured. In the case of a SaaS service, the CSP must inform the contracting party as soon as possible

of any future changes to the elements of the service which may result in a loss of functionality for the CSC.

SEC-8-SAFE-6. The CSP must document and implement measures to physically separate the service production environments from other environments, including development environments.

SEC-8-SAFE-7. The CSP must document and implement detection, prevention and recovery measures to protect against malicious code. The scope of application of this requirement on the service's IT system must include the user stations for which the CSP is responsible and the incoming flows on this same IT system.

SEC-8-SAFE-8. The CSP must document and implement awareness among its employees of the risks relating to malicious code and good practices to reduce the impact of an infection.

SEC-8-SAFE-9. The CSP must document and implement a policy for the backup and restoration of data for which it is responsible as part of the service. This policy must allow for a daily backup of all data (information, software, configurations, etc.) for which the CSP is responsible as part of the service. The CSP must document and implement backup protection measures in accordance with the access control policy (see dedicated chapter). This policy must include a monthly review of the backup access logs. The CSP must document and implement a procedure for regularly testing the restoration of backups. The CSP must locate the backups at a sufficient distance from the main equipment in accordance with the results of the risk assessment and in order to cope with major disasters. Backups are subject to the same location requirements as operational data. The backup site(s) are subject to the same security requirements as the main site, in particular those listed in the relevant chapters. Communication between the main site and the backup site must be protected by encryption, in accordance with the requirements of the relevant chapter.

SEC-8-SAFE-10. The CSP must document and implement a logging policy including as a minimum the following elements:

- The list of collection sources,
- The list of events to be logged by source,
- The purpose of the event logging,
- The frequency of collection and time base used,
- The local and centralised retention time,
- The log protection measures (including encryption and duplication),
- The location of the logs.

The CSP must generate and collect the following events:

- User activities related to information security,
- Changes to access rights within its area of responsibility,
- Events from anti-malware mechanisms,
- Changes to sensitive data,
- Exceptions,
- Failures,
- Any other event related to information security.

The CSP must retain the log events for a minimum of six months subject to compliance with legal and regulatory requirements. The CSP must provide, upon request from a contracting party, all events concerning said party.

SEC-8-SAFE-11. The CSP must protect the logging equipment and logged events against attacks on their availability, integrity or confidentiality. The CSP must manage the sizing of the storage space of all equipment hosting one or more collection sources in order to allow the local storage of logged events anticipated by the event logging policy. This sizing management must take into account changes to the IT system. The CSP must transfer the logged events, ensuring their confidentiality and integrity remains protected, to one or more dedicated central servers, and must store them on a physical machine separate from the one which generated them. The CSP must implement a backup of the collected events based on an appropriate policy. The CSP must perform the logging and event collection processes using accounts with necessary and sufficient privileges, and must limit access to logged events in accordance with the access control policy.

SEC-8-SAFE-12. The CSP must document and implement synchronisation of the clocks of all equipment to one or more internal time sources consistent with each other. These sources may themselves be synchronised with several reliable external sources, except for isolated networks. The CSP must implement time stamping of each logged event.

SEC-8-SAFE-13. The CSP must document and implement an infrastructure that allows the analysis and correlation of events recorded by the logging system in order to detect events that may affect the security of the service's IT system, in real time or subsequently for events up to six months old. The CSP must acknowledge the alarms raised by the event analysis and correlation infrastructure at least once a day.

SEC-8-SAFE-14. The CSP must document and implement a procedure for controlling the installation of software on the service's IT equipment. The CSP must document and implement a procedure for managing the configuration of the software environments made available to the CSC, in particular for keeping them secure.

SEC-8-SAFE-15. The CSP must document and implement a monitoring process to manage the technical vulnerabilities of the software and systems used in the service's IT system. The CSP must assess its exposure to these vulnerabilities by including them in the risk assessment and apply appropriate risk management measures.

SEC-8-SAFE-16. The CSP must document and implement a procedure requiring administrators for which it is responsible to use dedicated terminals for the exclusive performance of administrative tasks. Where the CSP authorises the mobility of administrators for which it is responsible, it must document this in a policy. The solution implemented must ensure that the level of security in this mobility scenario is at least equivalent to the level of security outside the mobility scenario.

SEC-8-SAFE-17. The CSP must specify all processes it supports to maintain data integrity, service continuity and data loss prevention specific to data import (e.g. pre- and post-transfer data backup and verification, downtime and secure transmission, roll back functionality and any testing functionality).

Requirements to ensure a "Trusted Cloud" level of trust

SEC-8-TRUSTED-18. The CSP must specify what, if any, security audit data can be imported (e.g. logs of user interactions with the cloud service that may be needed for security analysis and for monitoring requests).

2.9. COMMUNICATION SECURITY

Requirements to ensure a "Safe Cloud" level of trust

SEC-9-SAFE-1. The CSP must establish and keep updated a map of the service's IT system, linked to the asset inventory (see asset management chapter), including at least the following elements:

- The list of hardware or virtualised resources,
- The names and functions of the applications, supporting the service,
- The network architecture diagram at level 3 of the OSI model on which the nerve points are identified:
- The interconnection points, especially with third party and public networks,
- The networks, sub-networks, in particular administration networks,
- The equipment providing security functions (filtering, authentication, encryption, etc.),
- The servers hosting data or performing sensitive functions,
- The matrix of the authorised network flows, specifying:
- Their technical description (services, protocols and ports),
- The business line or infrastructure rationale,
- Where appropriate, where services, protocols or ports deemed insecure are used, the compensatory measures put in place, with a view to defence in depth.

The CSP must review the map at least once a year.

SEC-9-SAFE-2. The CSP must document and implement, for the service's IT system, partitioning measures (logical, physical or encryption) to separate network flows based on:

- The sensitivity of the information sent,
- The nature of the flows (production, administration, supervision, etc.),
- The domain to which the flows belong (of the CSCs - distinguished by CSC or all CSCs, of the CSP, of third parties, etc.),
- The technical field (processing, storage, etc.).

The CSP must partition all data flows internal to the service's IT system from any other IT system, either physically or by encryption. Where this partitioning is achieved by encryption, it shall be carried out in accordance with the requirements of the "cryptology" chapter. If the administration network of the technical infrastructure is not physically partitioned, the administration flows must pass through an encrypted tunnel, in accordance with the requirements of the "cryptology" chapter. The CSP must set up and configure an application firewall to protect the administrative interfaces for its CSCs that are exposed on a public network. The CSP must implement a filtering mechanism on all the administration and supervision interfaces of the service's technical infrastructure, authorising only the legitimate connections identified in the authorised flows matrix.

SEC-9-SAFE-3. The CSP must have one or more security incident detection probes on the service's IT system. These probes must, in particular, allow the supervision of each of the interconnections of the service's IT system with third-party IT systems and public networks. These probes must be collection sources for the event analysis and correlation infrastructure.

SEC-9-SAFE-4. The components used for data sharing must provide a sufficiently high degree of trust and security with regard to the integrity, confidentiality and availability of the information exchanged.

SEC-9-SAFE-5. The components used for data sharing check the authenticity and integrity of all system components before execution.

SEC-9-SAFE-6. The components used for data sharing record every access control decision, every access to data, every change to its configuration, and every instance in which a service receives fewer resources than requested as an integrity-protected log entry in its domain.

Requirements to ensure a "Trusted Cloud" level of trust

SEC-9-TRUSTED-7. When transferring data, the consumer and the data provider must each identify their organisation by means of unified digital identities.

SEC-9-TRUSTED-8. The consumer and the data provider must identify the components used for data sharing and processing via unified digital identities.

2.10. ACQUISITION, DEVELOPMENT AND MAINTENANCE OF IT SYSTEMS

Requirements to ensure a "Safe Cloud" level of trust

SEC-10-SAFE-1. The CSP must ensure the security of the information in the development cycle of IT systems.

SEC-10-SAFE-2. The CSP must document and implement rules for the secure development of software and systems, and apply them to internal developments.

SEC-10-SAFE-3. The CSP must document and implement appropriate training in secure development for the employees concerned.

SEC-10-SAFE-4. The CSP must document and implement a procedure for monitoring changes made to the service's IT system. The CSP must document and implement a procedure for validating changes made to the service's IT system on a pre-production environment before they go into production. The CSP must keep a history of the versions of the software and systems (internal or external developments, commercial products) implemented to enable a complete environment to be reconstituted, if necessary in a test environment, as it was implemented on a given date. The retention period of this history should be in line with the retention period of the backups.

SEC-10-SAFE-5. The CSP must document and implement a procedure for testing all applications before they go into production to ensure that there are no adverse effects on the activity or the security of the service.

SEC-10-SAFE-6. The CSP must implement a secure development environment to manage the entire development cycle of the service's IT system. The CSP must take into account the development environments in the risk assessment and ensure their protection in accordance with this reference document.

SEC-10-SAFE-7. The CSP must document and implement a procedure to supervise and control the outsourced software and systems development activity. This procedure must ensure that the outsourced development activity complies with the CSP's secure development policy and achieves a level of security for the external development equivalent to that of an internal development.

SEC-10-SAFE-8. The CSP must test new or updated IT systems for compliance and security functionality during development. It must document and implement a test procedure that identifies:

- The tasks to be carried out,
- The input data,
- The expected output results.

SEC-10-SAFE-9. The CSP must document and implement a procedure to ensure the integrity of the test data used in pre-production. If the CSP wishes to use the contracting party's data from production to carry out tests, it must first obtain the approval of the CSC and anonymise the data. The CSP must ensure the confidentiality of the data when it is anonymised.

SEC-10-SAFE-10. The CSP must ensure that the changes and configuration actions of the IT systems guarantee the security of the delivered cloud service.

2.11. RELATIONSHIP WITH THIRD PARTIES

Requirements to ensure a "Safe Cloud" level of trust

SEC-11-SAFE-1. The CSP must ensure the protection of the information that its providers can access, monitor agreed services and security requirements.

SEC-11-SAFE-2. The CSP must keep an up-to-date list of all third parties involved in the implementation of the service (host, developer, integrator, archiver, subcontractor operating on site or remotely, air-conditioning providers, etc.). This list must be exhaustive, specify the contribution of the third party to the service and to the processing of personal data, and take into account cases of multi-level subcontracting.

SEC-11-SAFE-3. The CSP must require third parties involved in the implementation of the service, in their contribution to the service, to maintain a level of security at least equivalent to that which it undertakes to maintain in its own security policy. This must be done through requirements, tailored to each third party and its contribution to the service, in the specifications or in the security clauses of the partnership agreements. The CSP must include these requirements in contracts with third parties. The CSP must contract, with each of the third parties involved in the implementation of the service, audit clauses allowing a qualification body to verify that these third parties comply with the requirements of this reference document. The CSP must define and assign roles and responsibilities for amending or terminating its contract with a third party involved in the implementation of the service.

SEC-11-SAFE-4. The CSP must document and implement a procedure to regularly monitor the measures put in place by third parties involved in the implementation of the service to meet the requirements of this reference document.

SEC-11-SAFE-5. The CSP must document and implement a procedure for monitoring changes made by third parties involved in the implementation of the service that may affect the level of security of the service's IT system. If a change to the third party involved in the implementation of the service affects the level of security of the service, the CSP must inform all CSCs without delay and implement measures to restore the previous level of security.

SEC-11-SAFE-6. The CSP must document and implement a procedure to review at least once a year the requirements for confidentiality or non-disclosure commitments relating to third parties involved in the implementation of the service.

2.12. MANAGEMENT OF INFORMATION SECURITY INCIDENTS

Requirements to ensure a "Safe Cloud" level of trust

SEC-12-SAFE-1. The CSP must document and implement a procedure for responding quickly and effectively to security incidents. These procedures must define the means and deadlines for communicating security incidents to all CSCs concerned and the level of confidentiality required for such communication. The CSP must inform its employees and all third parties involved in the implementation of the service of this procedure. The CSP must document any personal data breach and inform its CSC.

SEC-12-SAFE-2. The CSP must document and implement a procedure requiring its employees and third parties involved in the implementation of the service to report to them any known or suspected security incidents and breaches. The CSP must document and implement a procedure for all CSCs to report any known or suspected security incidents and vulnerabilities. The CSP must inform the CSC without delay of security incidents and the associated recommendations to limit their impact. It must allow the CSC to choose the severity level of the incidents they wish to be informed about. The CSP must report security incidents to the competent authorities in accordance with the applicable legal and regulatory requirements.

SEC-12-SAFE-3. The CSP must assess information security events and decide whether to classify them as security incidents. The assessment must be based on one or more scales (estimation, evaluation, etc.) shared with the CSC. Note: security incidents include personal data breaches. The CSP must use a classification to clearly identify security incidents involving CSC data, in accordance with the results of the risk assessment. This classification must include personal data breaches.

SEC-12-SAFE-4. The CSP must handle security incidents until they are resolved and must inform the CSC in accordance with the procedures. The CSP must archive documents detailing security incidents.

SEC-12-SAFE-5. The CSP must document and implement a continuous improvement process to reduce the occurrence and the impact of the types of security incidents already addressed.

SEC-12-SAFE-6. The CSP must document and implement a procedure for recording information about security incidents that can be used as evidence.

Requirements to ensure a "Trusted Cloud" level of trust

SEC-12-TRUSTED-7. The CSP must ensure a consistent and comprehensive approach to the identification, assessment, communication and escalation of security incidents.

2.13. BUSINESS CONTINUITY

Requirements to ensure a "Safe Cloud" level of trust

SEC-13-SAFE-1. The CSP must plan, implement, maintain and test business continuity and emergency management procedures and measures.

SEC-13-SAFE-2. The CSP must document, implement and keep updated a business continuity plan that takes into account information security.

SEC-13-SAFE-3. The CSP must document and implement procedures to maintain or restore the operation of the service and to ensure the availability of information at the level and within the timeframe to which the CSP has committed to the CSC in the service agreement.

SEC-13-SAFE-4. The CSP must document and implement a procedure for testing the business continuity plan to ensure that it is relevant and effective in a crisis situation.

SEC-13-SAFE-5. The CSP must document and implement measures to meet the service availability requirement defined in the CSA.

SEC-13-SAFE-6. In the event that the CSP is acquired by another entity, this entity will conclude all the rights and obligations of the CSP and the continuation of the services will be guaranteed by this entity for a period of at least 18 months from the date the service is taken over by the new entity.

SEC-13-SAFE-7. The CSP shall only delete CSC data from its systems after receiving explicit written approval from the CSC. In the event of the bankruptcy of the CSC, this approval must be given by the person responsible for the liquidation of the CSC.

2.14. COMPLIANCE

Requirements to ensure a "Safe Cloud" level of trust

SEC-14-SAFE-1. The CSP must ensure compliance with the legal, regulatory, self-imposed or contractual requirements for information security and compliance.

SEC-14-SAFE-2. The CSP must document and implement a three-year audit programme defining the scope and frequency of audits in accordance with change management, policies and the results of the risk assessment.

SEC-14-SAFE-3. The CSP, via the information security officer, must regularly ensure that all security procedures for which they are responsible are correctly executed to ensure compliance with security policies and standards.

SEC-14-SAFE-4. The CSP must document and implement a policy to check the technical compliance of the service with the requirements of this reference document. This policy must define the objectives, methods, frequencies, expected results and corrective measures.

3 REQUIREMENTS RELATED TO THE GENERAL DATA PROTECTION REGULATION (GDPR)

3.1. REGULATORY REQUIREMENTS

Requirements to ensure a "Safe Cloud" level of trust

RGPD-1-SAFE-1. The contract or any binding legal act between the CSP and the CSC must be compliant with the GDPR.

RGPD-1-SAFE-2. When the CSC uses the cloud services to process personal data, the CSP is a processor that must comply with all applicable obligations under the GDPR.

RGPD-1-SAFE-3. The infrastructure CSP shall ensure, with appropriate technical and/or organisational measures, that the cloud service is only provided after the conclusion of a contract with the CSC.

RGPD-1-SAFE-4. The contract between the infrastructure CSP and the CSC specifically sets out the respective roles and shared responsibilities of the CSP and the CSC with regard to security and data protection, as well as the technical configuration of the environment.

RGPD-1-SAFE-5. The legally binding contract establishes that data will only be processed on documented instructions from the CSC.

RGPD-1-SAFE-6. The CSP must inform the CSC immediately if, during the period of validity of the agreement, the data processing location changes from the one specified in the agreement for reasons within the CSP's area of responsibility.

RGPD-1-SAFE-7. The contract defines precisely whether and to what extent transfers of personal data to third countries will take place. Where appropriate, means are defined and implemented to protect data and comply with chapter V of the GDPR.

RGPD-1-SAFE-8. It is clearly defined whether and to what extent processors will be involved in the processing of personal data. Where appropriate, measures for their management should be put in place. This processing must be formally accepted by the cloud user beforehand. The list of processors involved at all levels must be communicated to the cloud user.

RGPD-1-SAFE-9. The obligation of the CSP to return the data media, return the data and delete the data upon completion of the processing must be stated in the contract or any legally binding agreement.

Requirements to ensure a "Trusted Cloud" level of trust

RGPD-1-TRUSTED-10. The contract must contain provisions for a customer audit right.

RGPD-1-TRUSTED-11. In the event of joint responsibility for processing between the CSP and the CSC, the contract must comply with Article 26 of the GDPR. In particular, the contract must provide for:

- Communication of the agreement to the people concerned,

- The designation of a contact point for the people concerned.

3.2. DATA PROTECTION

Requirements to ensure a "Safe Cloud" level of trust

RGPD-2-SAFE-1. The CSP must keep an up-to-date register of processing operations.

RGPD-2-SAFE-2. The purpose and duration of the processing must be described as specifically as possible in the legally binding agreement linked to the order.

RGPD-2-SAFE-3. The CSP only processes the personal data of the cloud user necessary to achieve the specified purposes of the processing.

RGPD-2-SAFE-4. The CSP is expressly prohibited from processing the personal data of cloud users for data mining, profiling or marketing purposes, and generally from accessing the personal data of the CSC, except as necessary for the provision of cloud services.

RGPD-2-SAFE-5. The CSP shall ensure that the processing of the personal data of the CSC is carried out only on the instructions of the CSC in accordance with the processing agreement.

RGPD-2-SAFE-6. The CSP must have its compliance with the personal data protection requirements assessed regularly by an independent and external third party.

RGPD-2-SAFE-7. The CSP shall ensure that its processors only act on the basis of a legally binding agreement in accordance with the agreement between the CSP and the CSC.

RGPD-2-SAFE-8. The CSP shall ensure the confidentiality, integrity and availability of the controller's personal data through the implementation of appropriate technical and/or organisational measures.

RGPD-2-SAFE-9. The CSP must provide the means for the CSC to provide individuals who request it with information about the processing of their personal data. With the means at its disposal, the CSC can send a copy of the personal data. The copy must be in a structured, commonly used, computer-readable format.

RGPD-2-SAFE-10. The CSP shall ensure, with appropriate measures, that the CSC has the possibility to rectify and complete incomplete personal data itself or to have it carried out by the CSP.

RGPD-2-SAFE-11. The CSP shall ensure that the CSC has the possibility to delete the personal data itself or to have it deleted by the CSP.

RGPD-2-SAFE-12. The CSP shall inform the CSC of personal data breaches and their extent without undue delay, using appropriate measures.

RGPD-2-SAFE-13. The GDPR provides that the transfer of such data to a third country may, in principle, only take place if the third country in question ensures an adequate level of protection for the data.

RGPD-2-SAFE-14. CHCs whose personal data is transferred to a third country on the basis of standard data protection clauses must enjoy a level of protection substantially equivalent to that guaranteed within the EU by this regulation, read in the light of the EU Charter.

RGPD-2-SAFE-15. In the absence of a decision on adequacy, the transfer can only take place if the exporter of the personal data, established in the EU, provides appropriate safeguards, which may include standard data protection clauses adopted by the Commission, and if the data subjects have enforceable rights and effective remedies.

RGPD-2-SAFE-16. The CSP must put in place effective mechanisms (standard protection clauses) to ensure that, in practice, the level of protection required by EU law is respected and that transfers of personal data based on such clauses are suspended or prohibited in the event of a breach of these clauses or if it is impossible to honour them.

RGPD-2-SAFE-17. The data exporter (CSC) and the transfer recipient (CSP) must first check that the level of protection required by EU law is respected in the third country concerned.

RGPD-2-SAFE-18. The recipient (CSP) must inform the exporter of the data (CSC) of its possible inability to comply with the standard protection clauses, and the latter (the customer) must then suspend the data transfer and/or terminate the contract with the former (the provider).

Requirements to ensure a "Trusted Cloud" level of trust

RGPD-2-TRUSTED-19. Where the CSP is required to appoint a data privacy officer (DPO), it must appoint this officer on the basis of professional qualities, knowledge of data protection law and practice, as well as on the basis of their ability to perform the tasks mentioned in Article 39 of the GDPR.

RGPD-2-TRUSTED-20. The technical and organisational measures are clearly defined based on the roles and responsibilities of the parties, including an adequate level of detail.

RGPD-2-TRUSTED-21. It is clearly defined how the CSC can meet its obligations, including through computerised means such as configuration tools or APIs.

RGPD-2-TRUSTED-22. The CSP shall ensure that the CSC has the possibility to restrict the processing of personal data themselves, or to have the restriction implemented by the CSP.

RGPD-2-TRUSTED-23. The CSP assists the CSC in carrying out their data protection impact study. If the CSP is aware of a high processing risk due to a data protection impact study carried out in advance by the CSC, the CSP must take measures appropriate to the risks.

4 REVERSIBILITY AND PORTABILITY REQUIREMENTS

4.1. PROCEDURAL REQUIREMENTS

Requirements to ensure a "Safe Cloud" level of trust

REV-1-SAFE-1. The CSP must provide the CSC with the procedures (and services) to initiate switching and porting from the cloud service when it is a porting source.

REV-1-SAFE-2. The CSP shall inform the CSC of the available terms for switching and porting to the cloud service.

REV-1-SAFE-3. The CSP must inform the CSC of the available porting methods and formats.

REV-1-SAFE-4. The CSP must provide the CSC with the fees and terms associated with the porting. Fees and terms must be clearly displayed at the subscription stage with warning mechanisms that inform the CSC of their ability to use reversibility services after a commitment phase.

REV-1-SAFE-5. The CSP must provide the CSC with the procedures for activating a new cloud service when it is the porting destination.

REV-1-SAFE-6. The CSP must provide the CSC with the process for exiting an existing cloud service, where it is the source of the porting and the CSC aims to terminate their use of the cloud service once the porting is complete. This process must be accompanied by a porting matrix on the scope of the target services and destination of the porting process.

REV-1-SAFE-7. The CSP must inform the CSC of its management capabilities for the porting and switching process.

Requirements to ensure a "Trusted Cloud" level of trust

REV-1-TRUSTED-8. The CSP must provide the CSC with (the services and) the procedures to initiate switching and porting to the cloud service when it is a porting destination.

REV-1-TRUSTED-9. The CSP must provide the CSC with the available standardised, documented, certified and secure porting methods and formats, including available safeguards and known restrictions and technical limitations.

REV-1-TRUSTED-10. The CSP must provide the CSC with the necessary management capabilities for the porting and switching process (e.g. end-to-end management to avoid loss of service for the customer).

4.2. PORTABILITY REQUIREMENTS

Requirements to ensure a "Safe Cloud" level of trust

REV-2-SAFE-1. The cloud service must be able to import and export CSC infrastructure artefacts in a simple and secure way, supporting the following scenarios: CSC to cloud service, cloud service to cloud

service and cloud service to CSC. The infrastructure CSP will provide the media to enable the transfer using a structured, commonly used and machine-readable format. This media must be documented for the different scenarios.

REV-2-SAFE-2. Where the CSC data involves infrastructure artefacts that rely on a cloud service functionality or capability, the infrastructure CSP must provide an appropriate description of the environment for their execution and how the service dependencies can be achieved. A portability impact matrix should indicate the dependencies to be considered during portability.

REV-2-SAFE-3. The CSP must make available to the CSC the operational procedures to transfer their data once the resolution of the source service is requested by the CSC.

Requirements to ensure a "Trusted Cloud" level of trust

REV-2-TRUSTED-4. The infrastructure CSP must take reasonable measures, minimising the impact on quality of service, to enable the CSC to maintain continuity of service while transferring data between providers, where technically possible.

REV-2-TRUSTED-5. The CSP must specify the period, defined and negotiated at the time of activation of the portability process, during which the CSC data will remain available for transfer once termination of the source service is requested by the CSC, and the nature of the clear and timely warnings issued prior to the deletion of the CSC data.

4.3. SCOPE AND COMPATIBILITY REQUIREMENTS

Requirements to ensure a "Safe Cloud" level of trust

REV-3-SAFE-1. The infrastructure CSP must describe in the Cloud infrastructure service provider's transparency statement the capabilities necessary for efficient cloud service switching, in order to minimise the loss of functionality, in particular the security functionality. It is recognised that the CSC and the infrastructure CSP will define in the infrastructure CSP's transparency statement which derived data will be subject to the same porting requirements. Any porting capabilities relating to data derived from the cloud service must be clearly described in the infrastructure CSP's transparency statement, but there is no requirement for the infrastructure CSP to support the porting of this data unless it is designated as part of the scope.

REV-3-SAFE-2. The CSP's transparency statement and contractual clauses must explicitly specify the following:

- The scope of the infrastructure artefacts available for transfer,
- Any claims of intellectual property rights that the infrastructure CSP has over the CSC data, and how these rights are enforced after a switchover.

4.4. PLANNING REQUIREMENTS

Requirements to ensure a "Safe Cloud" level of trust

REV-4-SAFE-1. The infrastructure CSP must provide the procedure for the CSC to test the transfer mechanisms and agree a transfer schedule, based on its business unit needs and security risks. The procedure must also specify the means that can be provided by the CSP in terms of support. Transfer testing must include both testing of the mechanisms used to port data to and from a cloud service and also the APIs used to access and manage the data when it is stored in the cloud service. Tests must be accepted with the CSC, as part of a transparent testing process. The CSC should be advised by the infrastructure CSP on further testing requirements.

REV-4-SAFE-2. The CSP must inform the CSC of the data migration schedule.

REV-4-SAFE-3. For the expected volume of Infrastructure Artefacts, the infrastructure CSP must provide the appropriate mechanisms, availability periods and transfer price. These elements must be displayed, known and accepted by the CSC as soon as the CSC signs the contract with the CSP.

REV-4-SAFE-4. The infrastructure CSP must provide the period of time during which the CSC data will remain available for transfer once termination of the source service is requested by the CSC, and the nature of the clear and timely warnings issued prior to the deletion of the CSC data. These elements must be displayed, known and accepted by the CSC as soon as the CSC signs the contract with the CSP.

Requirements to ensure a "Trusted Cloud" level of trust

REV-4-TRUSTED-5. The infrastructure CSP must provide a data migration schedule, integrated with portability reports with a duration contracted upfront, using current best practices and available technology, including non-networked solutions, in order to have a global view of end-to-end operations.

4.5. TRANSPARENCY REQUIREMENTS

Requirements to ensure a "Safe Cloud" level of trust

REV-5-SAFE-1. The terms and conditions necessary to comply with this reference document (including those referenced in clauses 5 of this Code) must be described to the potential CSC in clear terms and with an appropriate level of detail in a pre-contractual CSP transparency statement between the CSC and the infrastructure CSP. A contract template may be provided to the CSC to help them agree a contract with the CSPs. Please note that ensuring that pre-contractual information is available to potential CSCs does not require public disclosure and can be done on a confidential basis (e.g. via a non-disclosure agreement (NDA)).

REV-5-SAFE-2. The infrastructure CSP shall provide a transparency statement using the template of the SWIPO cloud IaaS and SaaS services CSP transparency statement version 1.0 and must not change the order and structure of this template. This transparency statement can be used as the basis for the contract template.

REV-5-SAFE-3. The description in the transparency statement must provide an appropriate level of detail, including:

- All aspects of compliance with this code,
- All documentation, the available support and tools to transfer CSC data from one infrastructure CSP to another,
- A description of the overall data porting process and capabilities supported, including any data backup and recovery processes adopted to protect data during data transfer, security measures, record management and, if agreed, the deletion of data from the CSC after successful porting (if the CSC intends to terminate the cloud service agreement). If the deletion capability is provided to the CSC by the infrastructure CSP, the CSC may perform the deletion themselves. The deletion must be performed by the source infrastructure CSP, if this capability is not provided to the CSC,
- The status and procedures for handling CSC data on the infrastructure of the infrastructure CSP after termination, including instructions from the CSC on any data retention, storage or restoration obligations stipulated by the applicable law or regulation,
- A clear description of all third parties that have access to the data through the process,
- A clear description of the policies and processes for accessing data in the event of bankruptcy of the infrastructure CSP or acquisition by another entity. These policies and processes must include informing the CSC without undue delay once bankruptcy proceedings have been initiated with the relevant public authorities,
- If a third party service provider is needed to convert, translate or transfer CSC infrastructure artefacts, this must be explicitly stated in the CSP transparency statement.

REV-5-SAFE-4. Before the CSC accepts the CSA, the infrastructure CSP must provide the CSC with a CSP transparency statement describing the mechanisms related to the porting of the CSC data:

- From the CSC's on-site facilities to the infrastructure CSP's cloud service,
- From another cloud service to a cloud service of the infrastructure CSP,
- And for the CSC's on-site facilities (from the infrastructure CSP's cloud service) to another cloud service from the infrastructure CSP, if they apply to CSC data, and how these aspects are addressed when considering data portability,
- Any related cost areas that would be billed by the infrastructure CSP. It must ensure that the information on data portability is made available to the CSC, including online and/or incorporated by reference in other contractual documents, and that the information is kept up-to-date.

REV-5-SAFE-5. The infrastructure CSP shall inform the CSC periodically and in a timely manner of any changes to the mechanisms and conditions, including identified costs, which would significantly alter the portability of the CSC's data. The CSC should have the right to terminate the agreement in advance.

REV-5-SAFE-6. The infrastructure CSP shall inform the CSC periodically and without undue delay of any permanent changes to its statement of adherence to the reference document.

4.6. PORTABILITY

Requirements to ensure a "Safe Cloud" level of trust

REV-6-SAFE-1. The infrastructure CSP must provide application programming interfaces related to the cloud service and, if provided, they must be fully documented. A catalogue of shared transfer APIs must be made available to the CSC by the CSP. These APIs must allow the transfer of infrastructure artefacts between participating parties. If there are code libraries or associated dependencies, they must be documented and made available.

REV-6-SAFE-2. The cloud service is not required by this trusted reference document to transform CSC infrastructure artefacts where the destination environment requires the infrastructure artefacts to be in different formats to those offered by the source environment. The parties may agree otherwise in the CSA.

REV-6-SAFE-3. The CSP must inform the CSC of the existence of an interface allowing them to perform data extractions.

REV-6-SAFE-4. The CSP must specify all processes, as part of the pre-contractual transparency document, to mention the use of subcontractors during the data portability activity.

REV-6-SAFE-5. The CSP must ensure that practices are in place to facilitate the switching of service providers and the porting of data in a structured, commonly used and machine-readable format, including open standard formats where required or requested by the service provider receiving the data. These elements must be incorporated into the contractual template of the CSC.

REV-6-SAFE-6. The CSP must ensure that pre-contractual information is available, with sufficiently detailed, clear and transparent information on data portability processes, technical requirements, time limits and fees in case a business user wishes to switch to another service provider or transfer data to their own IT systems. These elements must be incorporated into the contractual template of the CSC.

REV-6-SAFE-7. The CSP must specify all processes, as part of the pre-contractual transparency document, to mention the use of subcontractors during the data portability activity.

REV-6-SAFE-8. When exporting artefacts from the CSC to a cloud service, or between cloud services, the CSP must provide an FAQ to the CSC including elements for the user, administrator and business functions related to the cloud service.

REV-6-SAFE-9. The CSP must facilitate interoperability between CSC capabilities.

Requirements to ensure a "Trusted Cloud" level of trust

REV-6-TRUSTED-10. The infrastructure CSP must provide a self-service interface allowing the CSC to perform periodic data extractions from the CSC. This functionality can be contracted and may include additional costs. The operability of reversibility must be demonstrated and verified through periodic monitoring processes and at the initiative of the CSC.

REV-6-TRUSTED-11. When exporting artefacts from the CSC to a cloud service, or between cloud services, the CSP must provide support to facilitate interoperability between CSC capabilities, including the user, administrator and business functions related to the cloud service.

REV-6-TRUSTED-12. The CSP must allow access to the cloud service via other cloud services or IT systems of the CSCs, in order to obtain the stored data at the end of the contractual relationship and to securely delete it.

REV-6-TRUSTED-13. The CSP must declare any support facilitating interoperability between the CSC capabilities, including the user, administrator and business functions related to the cloud service.

4.7. SERVICE AGREEMENT

Requirements to ensure a "Safe Cloud" level of trust

REV-7-SAFE-1. The CSP must ensure the reversibility of the data using the technical methods at its disposal.

Requirements to ensure a "Trusted Cloud" level of trust

REV-7-TRUSTED-2. The CSP must ensure this reversibility through one of the following technical methods:

- The provision of files in one or more documented formats that can be used outside the service provided by the service provider;
- The implementation of technical interfaces allowing access to data through a documented and usable plan (API, pivot format, etc.).

The technical details of the reversibility are set out in the service agreement. These elements must be incorporated into the contractual template of the CSC.

4.8. EXPORTING DATA

Requirements to ensure a "Safe Cloud" level of trust

REV-8-SAFE-1. The CSP must specify the explicit and structured process for the export of data. It must include data management considerations (e.g. snapshots and phased approaches, record management policies and bandwidth assessment), all relevant timeframes, notification requirements, customer contact procedures (points of contact, escalation, etc.) and the impact on service continuity. This must include the availability of the data export process during and after the contractual period. This must also include the SLO and SQO of the SLA. The process and documentation must cover the technical, contractual and licensing issues in a way that is sufficient to enable porting and switching.

REV-8-SAFE-2. The CSP must contractually specify any obligations imposed before data export can commence.

REV-8-SAFE-3. The CSP must specify any known post-contractual licence fees or other commitments, such as patent and licence fees covering the use of derived data or data formats or claims and pending cases. These elements should be added to the impact matrix.

REV-8-SAFE-4. The CSP must specify any tools and services that incur additional costs for data export required by the source provider's processes for data portability, and provide continuous updating of tools and services. These elements should be added to the impact matrix.

REV-8-SAFE-5. The CSP must specify any tools or services provided (including, for example, support for integration or interoperability) that are available to assist the export process, and the costs associated with these tools. It must specify all third party tools or services in a portability catalogue.

REV-8-SAFE-6. The CSP must inform the CSC of its data portability processes and indicate the degree of autonomy of the CSC when exporting.

REV-8-SAFE-7. The CSP must specify which data, including derived data (e.g. calculated field values, graphs, displays) can be exported from the service before the actual export date.

REV-8-SAFE-8. The original CSP must specify any data access, retention periods and deletion processes (including notification of deletion), including the different categories of data (including derived data and management data) after expiry of the contract.

REV-8-SAFE-9. The CSP must specify the cost structure for the export of data and the associated procedures. It must provide sufficient transparency to allow the customer of the cloud service to calculate all data export charges levied by the provider.

REV-8-SAFE-10. The CSP must specify all processes it supports to maintain data integrity, service continuity and data loss prevention specific to data export (e.g. pre- and post-transfer data backup and verification, downtime and secure transmission, roll back functionality and any testing functionality).

REV-8-SAFE-11. The CSP must produce a reversibility matrix and specify known dependencies between the data to be exported and other data connected to another cloud service.

REV-8-SAFE-12. The CSP must specify the available mechanisms, protocols and interfaces that can be used to perform the data export (e.g. VPN LAN to LAN, Data Power, SFTP, HTTPS, API, physical media, etc.).

REV-8-SAFE-13. The CSP must specify what, if any, security audit data (e.g. access logs) is available for export (e.g. logs of user interactions with the cloud service that may be needed for security analysis and for monitoring requests).

REV-8-SAFE-14. The CSP must, where applicable, specify the encryption processes and services provided during data export (including unencrypted options) and describe how encryption keys are managed. The process must enable the CSC to decrypt the exported data.

REV-8-SAFE-15. The CSP must specify the security controls (e.g. access controls) available during data export.

Requirements to ensure a "Trusted Cloud" level of trust

REV-8-TRUSTED-16. The CSP must indicate whether or not its source processes for data portability allow the CSC to be completely independent when exporting data, i.e. when the customer does not need human interaction with the provider.

4.9. IMPORTING DATA

Requirements to ensure a "Safe Cloud" level of trust

REV-9-SAFE-1. The CSP must specify the explicit and structured process for the import of data. It must include data management considerations (e.g. snapshots and phased approaches, record management policies and bandwidth assessment), all relevant timeframes, notification requirements, customer contact procedures (points of contact, escalation, etc.) and the impact on service continuity. The process and documentation cover the technical, contractual and licensing issues in a way that is sufficient to enable porting and switching.

REV-9-SAFE-2. The CSP must specify all the tools required which entail additional costs for data import.

REV-9-SAFE-3. The CSP must specify any tools or services provided (including, for example, support for integration or interoperability) that are available to assist the import process, and the costs associated with these tools. It can specify any third party tools or services.

REV-9-SAFE-4. The CSP must specify whether or not the customer can be completely independent in importing data, i.e. where the customer of the cloud service does not need human interaction with the provider.

REV-9-SAFE-5. The CSP must specify which data, including data derived from a source export service (e.g. calculated field values, graphs, displays) can be imported into the service.

REV-9-SAFE-6. The CSP must specify the required format/structure of the imported data and where the definitions are available and under what terms (including industry or OpenSource formats (e.g. Open Financial Exchange format). The provider must specify all available validators and, if applicable, what type (e.g. structure, format, storage type, volume, links), from where and under what conditions. This must be sufficient to allow for porting and switching.

REV-9-SAFE-7. The CSP must specify the cost structure for importing data and the associated procedures (e.g. volume restrictions).

REV-9-SAFE-8. The CSP can specify any existing additional migration services (Cloud Provider or Third Party) and how they are available on the market.

REV-9-SAFE-9. The CSP must specify the notification processes and deadlines for users to be informed of any changes to the equipment included or referenced in its transparency statement.

REV-9-SAFE-10. The CSP must specify which encryption processes are used when importing data (including unencrypted options) and how encryption keys are managed.

REV-9-SAFE-11. The CSP must specify any obligations imposed before data import can commence.

4.10. STANDARDS AND OPENSOURCE

Requirements to ensure a “Safe Cloud” level of trust

REV-10-SAFE-1. The CSP must ensure that data standards are based on open market standards.

REV-10-SAFE-2. The CSP must specify the data standards, formats and/or types of files recommended, used or available for importing and exporting data (e.g. binary, MIME, CSV, SQL, JSON, XML, Avro) for each dataset available for import, including unstructured data.

REV-10-SAFE-3. The CSP must provide documentation on the format and structure of the exported data, including where it comes from, and under what conditions, if it comes from a third party (including industry or OpenSource formats (e.g. the Open Financial Exchange format)). This must be sufficient to allow for porting and switching.

REV-10-SAFE-4. The transfer of infrastructure artefacts from the CSC to and from the cloud service must use open standards and open protocols for the movement of infrastructure artefacts.

5 IMMUNITY REQUIREMENTS

5.1. TRANSPARENCY

Requirements to ensure a "Safe Cloud" level of trust

IMM-1-SAFE-1. The CSP must indicate the location of its assets, with the location accurate to city level.

IMM-1-SAFE-2. The CSP must indicate the measures implemented to deal with a service interruption situation.

IMM-1-SAFE-3. The CSP must clearly indicate the measures taken in case of bankruptcy.

IMM-1-SAFE-4. General provisions governing the rights of the parties to use the service and the data are formalised.

IMM-1-SAFE-5. An SLA is clearly defined.

IMM-1-SAFE-6. The CSP must indicate the measures implemented to govern changes of any kind, e.g. legal, technical, organisational.

IMM-1-SAFE-7. The CSP must include provisions governing copyright or other intellectual property rights.

5.2. DIGITAL SOVEREIGNTY

Requirements to ensure a "Safe Cloud" level of trust

IMM-2-SAFE-1. The CSP must report State investigation requests to the CSC.

Requirements to ensure a "Trusted Cloud" level of trust

IMM-2-TRUSTED-2. The CSP must ensure appropriate handling of State investigation requests, information to CSCs and limitations on access or disclosure of data.

5.3. ADDITIONAL REQUIREMENTS

Requirements to ensure a "Safe Cloud" level of trust

IMM-3-SAFE-1. The CSP must clearly indicate the location of its data centres.

IMM-3-SAFE-2. The CSP must indicate the list of companies (and their nationality) authorised to carry out audits.

IMM-3-SAFE-3. The CSP must display the list of legislation applicable to it that may have an impact on the CSC.

IMM-3-SAFE-4. The CSP must indicate the location of its registered offices.

IMM-3-SAFE-5. The CSP must list its shareholders and their location.

IMM-3-SAFE-6. The CSP must inform the CSC of the possibility of accessing the cloud service via other cloud services or IT systems of the CSC.

Requirements to ensure a "Trusted Cloud" level of trust

IMM-3-TRUSTED-7. The CSP must indicate the location of its subcontractors who may access the CSC data by any means.

IMM-3-TRUSTED-8. The CSP does not have any subcontractors outside the European Union who can access CSC data by any means.

IMM-3-TRUSTED-9. The jurisdictional competence for all service agreements of the CSP (with the CSC or with its subcontractors) is exclusively European.

IMM-3-TRUSTED-10. T Data must be processed and stored exclusively in the European Union.

IMM-3-TRUSTED-11. The audits are carried out by companies approved by European authorities (ANSSI, BSI, etc.).

IMM-3-TRUSTED-12. In the case where the Provider or subcontractor is subject to legal obligations to transmit or disclose data on the basis o f a non-EU statutory order, verified safeguards need to be in place that ensure that any access request is compliant with EU law.

IMM-3-TRUSTED-13. The CSP's registered head office, headquarters and main establishment shall be established in a Member State of the EU.

IMM-3-TRUSTED-14. Shareholders in the CSP, whose registered head office, headquarters and main establishment are not established in a Member State of the EU shall not, directly or indirectly, individually or jointly, hold control of the CSP. Control is defined as the ability of a natural or legal person to exercise decisive influence directly or indirectly on the CSP through one or more intermediate entities, de jure or de facto.

IMM-3-TRUSTED-15. In the event of recourse by the CSP, in the context of the services provided to the CSC, to the services of a third-party company - including a subcontractor - whose registered head office, headquarters and main establishment is outside of the European Union or who is owned or controlled directly or indirectly by another third-party company registered outside the European Union, the third-party company shall have no access over the CSC data[1] nor access and identity management for the services provided to the CSC. This includes, that the CSP, including any of its sub-processor, shall push back any request received from non-European authorities to obtain communication of personal data relating to European Customers, except if request is made in execution of a court judgment or order that is valid and legally binding under Union law and applicable member states law as provided by Article 48 GDPR.

IMM-3-TRUSTED-16. The CSP must guarantee continuous autonomy for all or part of the services it provides. The concept of operating autonomy shall be understood as the ability to maintain the

provision of the cloud computing service by drawing on the provider's own skills or by using adequate alternatives

IMM-3-TRUSTED-17. The service provided by the CSP must comply with existing fundamental rights legislation and Union values of respect for human dignity, freedom, equality, democracy and the rule of law. It may be taken into account for the assessment of the above-mentioned compliance, the fact that the provider has links with a foreign government or public body.

6 ENVIRONMENTAL FOCUS

This axis is to be considered as a collection of best practices and proposes an approach to achieve a high level of maturity on the environmental footprint of cloud services. The "trusted cloud" criteria are to be considered as targets to be reached, they are not discriminating as they stand. The objective is for users to be able to evaluate these criteria. In addition, some of the criteria may be amended at a later date, depending on the evolution of standards, norms or regulations, particularly at European level.

This fourth pillar on transparency and measurement of the cloud's environmental footprint is based on six main criteria.

6.1. ENERGY EFFICIENCY

Requirements to ensure a "Safe Cloud" level of trust

ENV-1-SAFE-1. The Cloud service providers provide their customers with energy efficiency data for each of their data centres.

ENV-1-SAFE-2. Cloud service providers report their carbon footprint metrics in CO2 emissions and with raw, non-compensated energy consumption data.

Requirements to ensure a "Trusted Cloud" level of trust

ENV-1-TRUSTED-3. Cloud service providers' data centres must meet a high standard of energy efficiency, such as the *EU Code of Conduct on Data Centre Energy Efficiency* [1]. Data centres operating at full capacity must meet an annual PUE (*Power Usage Effectiveness*[2]) target by 2030 of:

- 1.2 or less in cool climate regions;
- 1.3 or less in warm climate regions.

ENV-1-TRUSTED-4

. Cloud service providers' data centre components comply with eco-design standards. They indicate which standards/benchmark(s) are being followed.

6.2. CLEAN ENERGY (DECARBONISATION OF DATA CENTRE ACTIVITY)

Requirements to ensure a "Safe Cloud" level of trust

ENV-2-SAFE-1. Cloud service providers explain the different carbon offsetting mechanisms implemented to achieve carbon neutrality of their cloud activities and specify the timeframe for achieving carbon neutrality.

[1] https://e3p.jrc.ec.europa.eu/communities/data-centres-code-conduct
[2] The PUE is described in the standard ISO/IEC 30134-2:2016

ENV-2-SAFE-2. Cloud service providers disclose the geographical location of their emissions (Location-Based Emissions) and their use of low-carbon or renewable energy markets.

Requirements to ensure a "Trusted Cloud" level of trust

ENV-2-TRUSTED-3. The electricity production energy mix used by the networks that power cloud service providers' data centres ensure a carbon footprint of less than 100gCo2 eq / kWh.

6.3 WATER AND ABIOTIC RESOURCES: CONTROL OF WATER CONSUMPTION IN DATA CENTRES AND CONTROL OF WATER DISCHARGES AND WASTE

Requirements to ensure a "Safe Cloud" level of trust

ENV-3-SAFE-1. Cloud service providers detail their impact on the water resources needed to run their data centres.

ENV-3-SAFE 2. Cloud service providers report their annual Water Usage Effectiveness[3] (WUE) targets for their data centres.

ENV-3- SAFE 3. Cloud service providers indicate which cooling technique is used in their data centre (free cooling, free chilling …). The providers specify the temperature set point of the data centre.

ENV-3- SAFE 4. Cloud service providers specify the set of assumptions that enable them to calculate their environmental footprint, the depletion of non-renewable abiotic resources (mineral and fossil), the impact on water resources and on non-renewable primary energy.

6.4 CIRCULAR ECONOMY

Requirements to ensure a "Safe Cloud" level of trust

ENV-4-SAFE-1. Cloud service providers communicate their policy on sourcing, average lifespan, recycling and refurbishment of IT hardware embedded in their data centre and on their practices related to the circular economy.

ENV-4-SAFE-2. Cloud service providers are communicating on the full lifecycle impact of their infrastructures (data centres, servers, networks, …).

ENV-4-SAFE-3. Cloud Service Providers commit to comply at least with the Waste Electrical and Electronic Equipment (WEEE) recycling law.

ENV-4-SAFE-4. Cloud service providers commit to reporting lifespan information for their equipment and servers by 2025.

[3] Water Usage Effectiveness (WUE) is a metric developed by the Green Grid to measure data centre sustainability in terms of water usage and its relation to energy consumption. WUE is the ratio between the use of water in data centre systems (water loops, adiabatic towers, humidification, etc.) and the energy consumption of the IT equipment. The formula to calculate WUE is:
WUE = Data Centre Water Consumption (in liters) / IT Equipment Energy (in kilowatt hours)

ENV-4-SAFE-5. Cloud service providers communicate to each of their customers their numerical targets for the percentage of equipment and servers repaired, recycled or reused by 2025.

Requirements to ensure a "Trusted Cloud" level of trust

ENV-4-TRUSTED-6. Cloud service providers commit to promoting 100% reuse, repair or recycling of their used equipment and servers.

6.5 CIRCULAR ENERGY SYSTEM

Requirements to ensure a "Safe Cloud" level of trust

ENV-5-SAFE-1. Cloud service providers recover the waste heat produced by their data centres, where possible.

6.6 TRANSPARENCY AND AUDITABILITY OF MEASUREMENTS AND EMISSION FACTORS:

Requirements to ensure a "Safe Cloud" level of trust

ENV-6-SAFE-1. Cloud service providers transparently report their scope 1[4], scope 2[5] and scope 3[6] data with a publication of the full methodology, including the definition of the scopes, of their data centres outside the carbon offset strategy.

Requirements to ensure a "Trusted Cloud" level of trust

ENV-6-TRUSTED-2. Cloud service providers offer their customers a tool to measure their carbon impact by account (subscription, project, etc.), by service and by cloud region.

[4] Scope 1 covers all greenhouse gases emitted directly by the company: heating in the premises, emissions from company-owned vehicles, etc.
[5] Scope 2 includes indirect and energy-related emissions: these are emissions created during the production process.
[6] Scope 3 includes all indirect emissions, i.e. emissions related to upstream and downstream use: purchase of goods, purchase of services, use of services or products, etc.

Cigref
SUCCEED
WITH DIGITAL

Achieving digital success to help promote the economic growth and competitiveness of its members, who are major French corporations and public administrations, and users of digital solutions and services

Cigref is a network of major French corporations and public administrations set up in order to develop its members' ability to acquire and master digital technology. It is a unifying player in the digital society, thanks to its high-quality thinking and the extent to which it represents its members. Cigref is a not-for-profit body in accordance with the French law of 1901, created in 1970.
To achieve its mission, Cigref counts on three business units, which make it unique.

Belonging
Cigref speaks with one voice on behalf of major French corporations and public administrations on the subject of digital technology. Its members share their experiences of the use of technology in working groups in order to elicit best practices.

Intelligence
Cigref takes part in group discussions of the economic and societal issues raised by information technologies. Founded nearly 50 years ago, making it one of the oldest digital associations in France, it draws its legitimacy from both its history and its understanding of technical topics, giving it a solid platform of skills and know-how, the foundation stones of digital technology.

Influence
Cigref ensures that its member organisations' legitimate interests are known and respected. As an independent forum in which practitioners and actors can discuss and create, it is a benchmark recognised by its whole ecosystem.

www.cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr